

09/719056

Attorney Docket No. 450108-02448

JCO1 Rec'd PCT/PTO 06 DEC 2000

New Patent Application filed December 7, 2000, entitled:

**INFORMATION PROCESSING APPARATUS, INFORMATION  
PROCESSING METHOD, AND PROVIDING MEDIUM**

corresponding to PCT Application No. PCT/JP00/02288

filed April 7, 2000

Express Mail No.: EL585030171US

Date of Deposit: December 7, 2000

I hereby certify that this application and the accompanying papers are being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to:

Box PCT  
Assistant Commissioner for Patents  
Washington, D.C. 20231.



**This Page Blank (uspto)**

日本国特許庁  
PATENT OFFICE  
JAPANESE GOVERNMENT

09/7190388  
15.05.00

REC'D 26 MAY 2000

WIPO

PCT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日  
Date of Application:

1999年 4月 9日

出願番号  
Application Number:

平成11年特許願第103338号

出願人  
Applicant(s):

ソニー株式会社

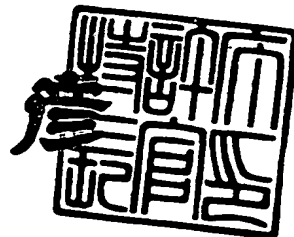
EKV

PRIORITY  
DOCUMENT  
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH RULE 17.1(a) OR (b)

2000年 3月10日

特許庁長官  
Commissioner,  
Patent Office

近藤 隆彦



出証番号 出証特2000-3015-8

【書類名】 特許願

【整理番号】 9900015512

【提出日】 平成11年 4月 9日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 12/16

【発明者】

    【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社  
内

    【氏名】 石橋 義人

【発明者】

    【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社  
内

    【氏名】 松山 科子

【発明者】

    【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社  
内

    【氏名】 大石 丈於

【発明者】

    【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社  
内

    【氏名】 武藤 明宏

【特許出願人】

    【識別番号】 000002185

    【氏名又は名称】 ソニー株式会社

    【代表者】 出井 伸之

【代理人】

    【識別番号】 100082131

    【弁理士】

    【氏名又は名称】 稲本 義雄



【電話番号】 03-3369-6479

【手数料の表示】

【予納台帳番号】 032089

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9708842

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報処理装置および方法、並びに提供媒体

【特許請求の範囲】

【請求項 1】 他の情報処理装置に接続され、暗号化されている情報を復号して利用する権利を購入する情報処理装置において、

購入した権利の内容を示す第 1 の利用内容、および前記第 1 の利用内容に対応する価格内容を特定する第 1 の使用許諾条件情報を作成する第 1 の作成手段と、

暗号化されている前記情報、前記第 1 の使用許諾条件情報、購入した前記権利の内容に基づいて再購入することができる権利の内容を示す第 2 の利用形式を含む取扱方針、前記第 2 の利用内容に対応する価格内容を含む価格情報、および暗号化されている前記情報を復号するために必要な鍵を記憶する記憶手段と、

前記他の情報処理装置を介して、権利の再購入が行われるとき、前記取扱方針と前記価格情報に基づいて、前記第 2 の利用内容、および前記第 2 の利用内容に対応する価格内容を特定する第 2 の使用許諾条件情報を作成する第 2 の作成手段と、

前記第 2 の作成手段により作成された前記第 2 の使用許諾条件情報、並びに前記記憶手段に記憶されている、暗号化されている前記情報および前記鍵を、前記他の情報処理装置に送信する送信手段と

を備えることを特徴とする情報処理装置。

【請求項 2】 前記第 2 の作成手段により作成された前記第 2 の使用許諾条件情報に基づいて、前記情報を利用するための処理を実行する第 1 の実行手段をさらに備えることを特徴とする請求項 1 に記載の情報処理装置。

【請求項 3】 前記第 1 の使用許諾条件情報および前記第 2 の使用許諾条件情報に対応する課金情報を作成する第 3 の作成手段と、

前記第 3 の作成手段により作成された前記課金情報に基づいて計上された課金を決済するための決済処理を実行する第 2 の実行手段と

をさらに備えることを特徴とする請求項 1 に記載の情報処理装置。

【請求項 4】 他の情報処理装置に接続され、暗号化されている情報を復号して利用する権利を購入する情報処理装置の情報処理方法において、

購入した権利の内容を示す第1の利用内容、および前記第1の利用内容に対応する価格内容を特定する第1の使用許諾条件情報を作成する第1の作成ステップと、

暗号化されている前記情報、前記第1の使用許諾条件情報、購入した前記権利の内容に基づいて再購入することができる権利の内容を示す第2の利用形式を含む取扱方針、前記第2の利用内容に対応する価格内容を含む価格情報、および暗号化されている前記情報を復号するために必要な鍵を記憶する記憶ステップと、

前記他の情報処理装置を介して、権利の再購入が行われるとき、前記取扱方針と前記価格情報に基づいて、前記第2の利用内容、および前記第2の利用内容に対応する価格内容を特定する第2の使用許諾条件情報を作成する第2の作成ステップと、

前記第2の作成ステップで作成された前記第2の使用許諾条件情報、並びに前記記憶ステップに記憶されている、暗号化されている前記情報および前記鍵を、前記他の情報処理装置に送信する送信ステップと

を含むことを特徴とする情報処理方法。

【請求項5】 他の情報処理装置に接続され、暗号化されている情報を復号して利用する権利を購入する情報処理装置に、

購入した権利の内容を示す第1の利用内容、および前記第1の利用内容に対応する価格内容を特定する第1の使用許諾条件情報を作成する第1の作成ステップと、

暗号化されている前記情報、前記第1の使用許諾条件情報、購入した前記権利の内容に基づいて再購入することができる権利の内容を示す第2の利用形式を含む取扱方針、前記第2の利用内容に対応する価格内容を含む価格情報、および暗号化されている前記情報を復号するために必要な鍵を記憶する記憶ステップと、

前記他の情報処理装置を介して、権利の再購入が行われるとき、前記取扱方針と前記価格情報に基づいて、前記第2の利用内容、および前記第2の利用内容に対応する価格内容を特定する第2の使用許諾条件情報を作成する第2の作成ステップと、

前記第2の作成ステップで作成された前記第2の使用許諾条件情報、並びに前

記記憶ステップに記憶されている、暗号化されている前記情報および前記鍵を、前記他の情報処理装置に送信する送信ステップと

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする提供媒体。

【請求項 6】 他の情報処理装置に接続され、購入された権利に対応して、暗号化されている情報を復号して利用する情報処理装置において、

前記他の情報処理装置から送信されてきた、暗号化されている前記情報、暗号化されている前記情報を復号するために必要な鍵、および前記権利の内容を示す利用内容と前記利用内容に対応する価格内容を特定する使用許諾条件情報を受信する受信手段と、

前記使用許諾条件情報により特定される前記利用内容に示される前記権利の内容に基づいて、前記情報を利用するための処理を実行する実行手段と

を備えることを特徴とする情報処理装置。

【請求項 7】 他の情報処理装置に接続され、購入された権利に対応して、暗号化されている情報を復号して利用する情報処理装置の情報処理方法において

前記他の情報処理装置から送信されてきた、暗号化されている前記情報、暗号化されている前記情報を復号するために必要な鍵、および前記権利の内容を示す利用内容と前記利用内容に対応する価格内容を特定する使用許諾条件情報を受信する受信ステップと、

前記使用許諾条件情報により特定される前記利用内容に示される前記権利の内容に基づいて、前記情報を利用するための処理を実行する実行ステップと

を含むことを特徴とする情報処理方法。

【請求項 8】 他の情報処理装置に接続され、購入された権利に対応して、暗号化されている情報を復号して利用する情報処理装置に、

前記他の情報処理装置から送信されてきた、暗号化されている前記情報、暗号化されている前記情報を復号するために必要な鍵、および前記権利の内容を示す利用内容と前記利用内容に対応する価格内容を特定する使用許諾条件情報を受信する受信ステップと、

前記使用許諾条件情報により特定される前記利用内容に示される前記権利の内容に基づいて、前記情報を利用するための処理を実行する実行ステップと

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする提供媒体。

【請求項 9】 他の情報処理装置に接続され、暗号化されている情報を復号して利用する権利を購入する情報処理装置において、

暗号化されている前記情報、購入することができる権利の内容を示す利用内容を含む取扱方針、前記利用内容に対応する価格内容を含む価格情報、および暗号化されている前記情報を復号するために必要な鍵を記憶する記憶手段と、

前記記憶手段に記憶されている前記取扱方針および前記価格情報に基づいて、前記利用内容、および前記利用内容に対応する価格内容を特定する使用許諾条件情報を作成する作成手段と、

前記他の情報処理装置において、権利の再購入が行われるとき、前記作成手段により作成された前記使用許諾条件情報、並びに前記記憶手段に記憶されている、暗号化されている前記情報および前記鍵を、前記他の情報処理装置に送信する送信手段と

を備えることを特徴とする情報処理装置。

【請求項 10】 他の情報処理装置に接続され、暗号化されている情報を復号して利用する権利を購入する情報処理装置の情報処理方法において、

暗号化されている前記情報、購入することができる権利の内容を示す利用内容を含む取扱方針、前記利用内容に対応する価格内容を含む価格情報、および暗号化されている前記情報を復号するために必要な鍵を記憶する記憶ステップと、

前記記憶ステップで記憶された前記取扱方針および前記価格情報に基づいて、前記利用内容、および前記利用内容に対応する価格内容を特定する使用許諾条件情報を作成する作成ステップと、

前記他の情報処理装置において、権利の再購入が行われるとき、前記作成ステップで作成された前記使用許諾条件情報、並びに前記記憶ステップで記憶された、暗号化されている前記情報および前記鍵を、前記他の情報処理装置に送信する送信ステップと

を含むことを特徴とする情報処理方法。

【請求項 11】 他の情報処理装置に接続され、暗号化されている情報を復号して利用する権利を購入する情報処理装置に、

暗号化されている前記情報、購入することができる権利の内容を示す利用内容を含む取扱方針、前記利用内容に対応する価格内容を含む価格情報、および暗号化されている前記情報を復号するために必要な鍵を記憶する記憶ステップと、

前記記憶ステップで記憶された前記取扱方針および前記価格情報に基づいて、前記利用内容、および前記利用内容に対応する価格内容を特定する使用許諾条件情報を作成する作成ステップと、

前記他の情報処理装置において、権利の再購入が行われるとき、前記作成ステップにて作成された前記使用許諾条件情報、並びに前記記憶ステップに記憶されている、暗号化されている前記情報および前記鍵を、前記他の情報処理装置に送信する送信ステップと

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする提供媒体。

【請求項 12】 他の情報処理装置に接続され、購入した権利に対応して、暗号化されている情報を復号して利用する情報処理装置において、

前記他の情報処理装置から送信されてきた、暗号化されている前記情報、暗号化されている前記情報を復号するために必要な鍵、および所定の権利の内容を示す第 1 の利用形式、および前記第 1 の利用形式に対応する価格内容を特定する使用許諾条件情報を受信する受信手段と、

前記受信手段により受信された前記使用許諾条件情報により特定される前記第 1 の利用内容に示される前記権利の内容に基づいて再購入される権利の内容を示す第 2 の利用内容を含む取扱方針、および前記第 2 の利用内容に対応する価格内容を含む価格情報を記憶する記憶手段と、

前記記憶手段に記憶されている前記取扱方針および前記価格情報に基づいて、前記第 2 の利用内容、および前記第 2 の利用内容に対応する価格内容を特定する第 2 の使用許諾条件情報を作成する第 1 の作成手段と

を備えることを特徴とする情報処理装置。

【請求項 13】 前記第 1 の作成手段により作成された前記第 2 の使用許諾条件情報に対応する課金情報を作成する第 2 の作成手段と、

前記第 2 の作成手段により作成された前記課金情報に基づいて計上された課金を決済するための決済処理を実行する実行手段と

をさらに備えることを特徴とする請求項 12 に記載の情報処理装置。

【請求項 14】 他の情報処理装置に接続され、購入した権利に対応して、暗号化されている情報を復号して利用する情報処理装置の情報処理方法において

前記他の情報処理装置から送信されてきた、暗号化されている前記情報、暗号化されている前記情報を復号するために必要な鍵、および所定の権利の内容を示す第 1 の利用形式、および前記第 1 の利用形式に対応する価格内容を特定する使用許諾条件情報を受信する受信ステップと、

前記受信ステップで受信された前記使用許諾条件情報により特定される前記第 1 の利用内容に示される前記権利の内容に基づいて再購入される権利の内容を示す第 2 の利用内容を含む取扱方針、および前記第 2 の利用内容に対応する価格内容を含む価格情報を記憶する記憶ステップと、

前記記憶ステップで記憶された前記取扱方針および前記価格情報に基づいて、前記第 2 の利用内容、および前記第 2 の利用内容に対応する価格内容を特定する第 2 の使用許諾条件情報を作成する第 1 の作成ステップと

を含むことを特徴とする情報処理方法。

【請求項 15】 他の情報処理装置に接続され、購入した権利に対応して、暗号化されている情報を復号して利用する情報処理装置に、

前記他の情報処理装置から送信されてきた、暗号化されている前記情報、暗号化されている前記情報を復号するために必要な鍵、および所定の権利の内容を示す第 1 の利用形式、および前記第 1 の利用形式に対応する価格内容を特定する使用許諾条件情報を受信する受信ステップと、

前記受信ステップで受信された前記使用許諾条件情報により特定される前記第 1 の利用内容に示される前記権利の内容に基づいて再購入される権利の内容を示す第 2 の利用内容を含む取扱方針、および前記第 2 の利用内容に対応する価格内容

を含む価格情報を記憶する記憶ステップと、

前記記憶ステップで記憶された前記取扱方針および前記価格情報に基づいて、前記第 2 の利用内容、および前記第 2 の利用内容に対応する価格内容を特定する第 2 の使用許諾条件情報を作成する第 1 の作成ステップと

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする提供媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、情報処理装置および方法、並び提供媒体に関し、特に、暗号化された情報を利用する情報処理装置および方法、並びに提供媒体に関する。

【0002】

【従来の技術】

音楽などの情報（以下、コンテンツと称する）を暗号化し、所定の契約を交わしたユーザの情報処理装置に送信し、ユーザが、情報処理装置でコンテンツを復号して、利用するシステムがある。

【0003】

【発明が解決しようとする課題】

ユーザが複数の情報処理装置を有している場合、そのユーザは、それぞれの情報処理装置毎に、コンテンツを購入し、その利用料金を支払わなければならない。すなわち、一度購入したコンテンツであっても、異なる情報処理装置においてそれを利用する場合（購入する場合）、同一の料金で、再度購入する必要がある。

【0004】

本発明はこのような状況に鑑みてなされたものであり、同一のコンテンツを再購入する場合、ユーザが、割引料金で、購入することができるようにするものである。

【0005】

【課題を解決するための手段】



請求項 1 に記載の情報処理装置は、購入した権利の内容を示す第 1 の利用内容、および第 1 の利用内容に対応する価格内容を特定する第 1 の使用許諾条件情報を作成する第 1 の作成手段と、暗号化されている情報、第 1 の使用許諾条件情報、購入した権利の内容に基づいて再購入することができる権利の内容を示す第 2 の利用形式を含む取扱方針、第 2 の利用内容に対応する価格内容を含む価格情報、および暗号化されている情報を復号するために必要な鍵を記憶する記憶手段と、他の情報処理装置を介して、権利の再購入が行われるとき、取扱方針と価格情報に基づいて、第 2 の利用内容、および第 2 の利用内容に対応する価格内容を特定する第 2 の使用許諾条件情報を作成する第 2 の作成手段と、第 2 の作成手段により作成された第 2 の使用許諾条件情報、並びに記憶手段に記憶されている、暗号化されている情報および鍵を、他の情報処理装置に送信する送信手段とを備えることを特徴とする。

## 【0006】

請求項 4 に記載の情報処理方法は、購入した権利の内容を示す第 1 の利用内容、および第 1 の利用内容に対応する価格内容を特定する第 1 の使用許諾条件情報を作成する第 1 の作成ステップと、暗号化されている情報、第 1 の使用許諾条件情報、購入した権利の内容に基づいて再購入することができる権利の内容を示す第 2 の利用形式を含む取扱方針、第 2 の利用内容に対応する価格内容を含む価格情報、および暗号化されている情報を復号するために必要な鍵を記憶する記憶ステップと、他の情報処理装置を介して、権利の再購入が行われるとき、取扱方針と価格情報に基づいて、第 2 の利用内容、および第 2 の利用内容に対応する価格内容を特定する第 2 の使用許諾条件情報を作成する第 2 の作成ステップと、第 2 の作成ステップで作成された第 2 の使用許諾条件情報、並びに記憶ステップに記憶されている、暗号化されている情報および鍵を、他の情報処理装置に送信する送信ステップとを含むことを特徴とする。

## 【0007】

請求項 5 に記載の提供媒体は、購入した権利の内容を示す第 1 の利用内容、および第 1 の利用内容に対応する価格内容を特定する第 1 の使用許諾条件情報を作成する第 1 の作成ステップと、暗号化されている情報、第 1 の使用許諾条件情報

、購入した権利の内容に基づいて再購入することができる権利の内容を示す第2の利用形式を含む取扱方針、第2の利用内容に対応する価格内容を含む価格情報、および暗号化されている情報を復号するために必要な鍵を記憶する記憶ステップと、他の情報処理装置を介して、権利の再購入が行われるとき、取扱方針と価格情報に基づいて、第2の利用内容、および第2の利用内容に対応する価格内容を特定する第2の使用許諾条件情報を作成する第2の作成ステップと、第2の作成ステップで作成された第2の使用許諾条件情報、並びに記憶ステップに記憶されている、暗号化されている情報および鍵を、他の情報処理装置に送信する送信ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

## 【0008】

請求項1に記載の情報処理装置、請求項4に記載の情報処理方法、および請求項5に記載の提供媒体においては、購入された権利の内容を示す第1の利用内容、および第1の利用内容に対応する価格内容を特定する第1の使用許諾条件情報が作成され、暗号化されている情報、第1の使用許諾条件情報、購入した権利の内容に基づいて再購入することができる権利の内容を示す第2の利用形式を含む取扱方針、第2の利用内容に対応する価格内容を含む価格情報、および暗号化されている情報を復号するために必要な鍵が記憶され、他の情報処理装置を介して、権利の再購入が行われるとき、取扱方針と価格情報に基づいて、第2の利用内容、および第2の利用内容に対応する価格内容を特定する第2の使用許諾条件情報が作成され、作成された第2の使用許諾条件情報、並びに記憶手段に記憶されている、暗号化されている情報および鍵が、他の情報処理装置に送信される。

## 【0009】

請求項6に記載の情報処理装置は、他の情報処理装置から送信されてきた、暗号化されている情報、暗号化されている情報を復号するために必要な鍵、および権利の内容を示す利用内容と利用内容に対応する価格内容を特定する使用許諾条件情報を受信する受信手段と、使用許諾条件情報により特定される利用内容に示される権利の内容に基づいて、情報を利用するための処理を実行する実行手段とを備えることを特徴とする。

## 【0010】

請求項7に記載の情報処理方法は、他の情報処理装置から送信されてきた、暗号化されている情報、暗号化されている情報を復号するために必要な鍵、および権利の内容を示す利用内容と利用内容に対応する価格内容を特定する使用許諾条件情報を受信する受信ステップと、使用許諾条件情報により特定される利用内容に示される権利の内容に基づいて、情報を利用するための処理を実行する実行ステップとを含むことを特徴とする。

## 【0011】

請求項8に記載の提供媒体は、他の情報処理装置から送信されてきた、暗号化されている情報、暗号化されている情報を復号するために必要な鍵、および権利の内容を示す利用内容と利用内容に対応する価格内容を特定する使用許諾条件情報を受信する受信ステップと、使用許諾条件情報により特定される利用内容に示される権利の内容に基づいて、情報を利用するための処理を実行する実行ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

## 【0012】

請求項6に記載の情報処理装置、請求項7に記載の情報処理方法、および請求項8に記載の提供媒体においては、他の情報処理装置から送信されてきた、暗号化されている情報、暗号化されている情報を復号するために必要な鍵、および権利の内容を示す利用内容と利用内容に対応する価格内容を特定する使用許諾条件情報が受信され、使用許諾条件情報により特定される利用内容に示される権利の内容に基づいて、情報を利用するための処理が実行される。

## 【0013】

請求項9に記載の情報処理装置は、暗号化されている情報、購入することができ権利の内容を示す利用内容を含む取扱方針、利用内容に対応する価格内容を含む価格情報、および暗号化されている情報を復号するために必要な鍵を記憶する記憶手段と、記憶手段に記憶されている取扱方針および価格情報に基づいて、利用内容、および利用内容に対応する価格内容を特定する使用許諾条件情報を作成する作成手段と、他の情報処理装置において、権利の再購入が行われるとき、

作成手段により作成された使用許諾条件情報、並びに記憶手段に記憶されている、暗号化されている情報および鍵を、他の情報処理装置に送信する送信手段とを備えることを特徴とする。

【0014】

請求項10に記載の情報処理方法は、暗号化されている情報、購入することができる権利の内容を示す利用内容を含む取扱方針、利用内容に対応する価格内容を含む価格情報、および暗号化されている情報を復号するために必要な鍵を記憶する記憶ステップと、記憶ステップで記憶された取扱方針および価格情報に基づいて、利用内容、および利用内容に対応する価格内容を特定する使用許諾条件情報を作成する作成ステップと、他の情報処理装置において、権利の再購入が行われるとき、作成ステップで作成された使用許諾条件情報、並びに記憶ステップで記憶された、暗号化されている情報および鍵を、他の情報処理装置に送信する送信ステップとを含むことを特徴とする。

【0015】

請求項11に記載の提供媒体は、暗号化されている情報、購入することができる権利の内容を示す利用内容を含む取扱方針、利用内容に対応する価格内容を含む価格情報、および暗号化されている情報を復号するために必要な鍵を記憶する記憶ステップと、記憶ステップで記憶された取扱方針および価格情報に基づいて、利用内容、および利用内容に対応する価格内容を特定する使用許諾条件情報を作成する作成ステップと、他の情報処理装置において、権利の再購入が行われるとき、作成ステップで作成された使用許諾条件情報、並びに記憶ステップで記憶された、暗号化されている情報および鍵を、他の情報処理装置に送信する送信ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

【0016】

請求項9に記載の情報処理装置、請求項10に記載の情報処理方法、および請求項11に記載の提供媒体においては、暗号化されている情報、購入することができる権利の内容を示す利用内容を含む取扱方針、利用内容に対応する価格内容を含む価格情報、および暗号化されている情報を復号するために必要な鍵が記憶

され、記憶された取扱方針および価格情報に基づいて、利用内容、および利用内容に対応する価格内容を特定する使用許諾条件情報が作成され、他の情報処理装置において、権利の再購入が行われるとき、作成された使用許諾条件情報、並びに記憶された、暗号化されている情報および鍵が、他の情報処理装置に送信される。

【0017】

請求項12に記載の情報処理装置は、他の情報処理装置から送信されてきた、暗号化されている情報、暗号化されている情報を復号するために必要な鍵、および所定の権利の内容を示す第1の利用形式、および第1の利用形式に対応する価格内容を特定する使用許諾条件情報を受信する受信手段と、受信手段により受信された使用許諾条件情報により特定される第1の利用内容に示される権利の内容に基づいて再購入される権利の内容を示す第2の利用内容を含む取扱方針、および第2の利用内容に対応する価格内容を含む価格情報を記憶する記憶手段と、記憶手段に記憶されている取扱方針および価格情報に基づいて、第2の利用内容、および第2の利用内容に対応する価格内容を特定する第2の使用許諾条件情報を作成する第1の作成手段とを備えることを特徴とする。

【0018】

請求項14に記載の情報処理方法は、他の情報処理装置から送信されてきた、暗号化されている情報、暗号化されている情報を復号するために必要な鍵、および所定の権利の内容を示す第1の利用形式、および第1の利用形式に対応する価格内容を特定する使用許諾条件情報を受信する受信ステップと、受信ステップで受信された使用許諾条件情報により特定される第1の利用内容に示される権利の内容に基づいて再購入される権利の内容を示す第2の利用内容を含む取扱方針、および第2の利用内容に対応する価格内容を含む価格情報を記憶する記憶ステップと、記憶ステップで記憶された取扱方針および価格情報に基づいて、第2の利用内容、および第2の利用内容に対応する価格内容を特定する第2の使用許諾条件情報を作成する作成ステップとを含むことを特徴とする。

【0019】

請求項15に記載の提供媒体は、他の情報処理装置から送信されてきた、暗号

化されている情報、暗号化されている情報を復号するために必要な鍵、および所定の権利の内容を示す第1の利用形式、および第1の利用形式に対応する価格内容を特定する使用許諾条件情報を受信する受信ステップと、受信ステップで受信された使用許諾条件情報により特定される第1の利用内容に示される権利の内容に基づいて再購入される権利の内容を示す第2の利用内容を含む取扱方針、および第2の利用内容に対応する価格内容を含む価格情報を記憶する記憶ステップと、記憶ステップで記憶された取扱方針および価格情報に基づいて、第2の利用内容、および第2の利用内容に対応する価格内容を特定する第2の使用許諾条件情報を作成する作成ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

#### 【0020】

請求項12に記載の情報処理装置、請求項14に記載の情報処理方法、および請求項15に記載の提供媒体においては、他の情報処理装置から送信されてきた、暗号化されている情報、暗号化されている情報を復号するために必要な鍵、および所定の権利の内容を示す第1の利用形式、および第1の利用形式に対応する価格内容を特定する使用許諾条件情報が受信され、受信された使用許諾条件情報により特定される第1の利用内容に示される権利の内容に基づいて再購入される権利の内容を示す第2の利用内容を含む取扱方針、および第2の利用内容に対応する価格内容を含む価格情報が記憶され、記憶された取扱方針および価格情報に基づいて、第2の利用内容、および第2の利用内容に対応する価格内容を特定する第2の使用許諾条件情報が作成される。

#### 【0021】

##### 【発明の実施の形態】

以下に本発明の実施の形態を説明するが、特許請求の範囲に記載の発明の各手段と以下の実施の形態との対応関係を明らかにするために、各手段の後の括弧内に、対応する実施の形態（但し一例）を付加して本発明の特徴を記述すると、次のようになる。但し勿論この記載は、各手段を記載したものに限定することを意味するものではない。

#### 【0022】

図1は、本発明を適用したEMD(Electronic Music Distribution:電子音楽配信)システムを説明する図である。EMDシステムは、各装置を管理するEMDサービスセンタ1、コンテンツを提供するコンテンツプロバイダ2、コンテンツに対応する所定のサービスを提供するサービスプロバイダ3、およびコンテンツが利用される機器(この例の場合、レシーバ51、レシーバ201、およびレシーバ301)からなるユーザネットワーク5から構成されている。

【0023】

EMDシステムにおけるコンテンツ(Content)とは、情報そのものが価値を有するデジタルデータで、この例の場合、1つのコンテンツは、1曲分の音楽データに相当する。

【0024】

EMDサービスセンタ1は、EMDシステムにおける主な情報の流れを示す図2に示すように、ユーザホームネットワーク5およびコンテンツプロバイダ2に、コンテンツを利用するために必要な配送用鍵Kdを送信する。EMDサービスセンタ1はまた、ユーザホームネットワーク5の機器から、課金情報等を受信して、料金を精算する処理などを実行する。

【0025】

コンテンツプロバイダ2は、提供するコンテンツ(コンテンツ鍵Kcoで暗号化されている)、そのコンテンツを復号するために必要なコンテンツ鍵Kco(配送用鍵Kdで暗号化されている)、およびコンテンツの利用内容などを示す取扱方針(以下、UCP(Usage Control Policy)と記述する)を保持し、それらを、コンテンツプロバイダセキュアコンテナ(後述)と称する形態で、サービスプロバイダ3に供給する。

【0026】

サービスプロバイダ3は、コンテンツプロバイダ2から供給されるUCPの利用内容に対応して、1つまたは複数の価格情報(以下、PT(Price Tag)と記述する)を作成する。サービスプロバイダ3は、作成したPTを、コンテンツプロバイダ2から供給されたコンテンツ(コンテンツ鍵Kcoで暗号化されている)、コンテンツ鍵Kco(配送用鍵Kdで暗号化されている)、およびUCPとともに、サ

ービスプロバイダセキュアコンテナと称する形態で、専用のケーブルネットワーク、インターネット、または衛星通信などから構成されるネットワーク4を介して、ユーザホームネットワーク5に送信する。

【0027】

ユーザホームネットワーク5は、供給されたUCPおよびPTに基づいて、使用許諾条件情報（以下、UCS(Usage Control Status)と称する）を作成し、作成したUCSに基づいてコンテンツを利用する処理を実行する。ユーザホームネットワーク5はまた、UCSを作成するタイミングで課金情報を作成し、例えば、配送用鍵Kdの供給を受けるタイミングで、対応するUCPおよびPTなどとともにEMDサービスセンタ1に送信する。

【0028】

図3は、EMDサービスセンタ1の機能的構成を示すブロック図である。サービスプロバイダ管理部11は、サービスプロバイダ3に利益分配の情報を供給する。コンテンツプロバイダ管理部12は、コンテンツプロバイダ2に配送用鍵Kdを送信したり、利益分配の情報を供給する。

【0029】

著作権管理部13は、ユーザホームネットワーク5のコンテンツの利用の実績を示す情報を、著作権を管理する団体、例えば、JASRAC(Japanese Society for Rights of Authors, Composers and Publishers:日本音楽著作権協会)に送信する。

【0030】

鍵サーバ14は、配送用鍵Kdを記憶しており、それを、コンテンツプロバイダ管理部12を介してコンテンツプロバイダ2に供給したり、ユーザ管理部18等を介してユーザホームネットワーク5に供給する。

【0031】

ユーザホームネットワーク5の機器およびコンテンツプロバイダ2に供給される、EMDサービスセンタ1からの配送用鍵Kdについて、図4乃至図7を参照して説明する。



## 【0032】

図4は、コンテンツプロバイダ2がコンテンツの提供を開始し、ユーザホームネットワーク5を構成するレシーバ51がコンテンツの利用を開始する、1998年1月における、EMDサービスセンタ1が有する配送用鍵Kd、コンテンツプロバイダ2が有する配送用鍵Kd、およびレシーバ51が有する配送用鍵Kdを示す図である。

## 【0033】

図4の例において、配送用鍵Kdは、暦の月の初日から月の末日まで、使用可能であり、たとえば、所定のビット数の乱数である”aaaaaaaa”の値を有するバージョン1である配送用鍵Kdは、1998年1月1日から1998年1月31日まで使用可能（すなわち、1998年1月1日から1998年1月31日の期間にサービスプロバイダ3を介してユーザホームネットワーク5に配布されるコンテンツを暗号化するコンテンツ鍵Kcoは、バージョン1である配送用鍵Kdで暗号化されている）であり、所定のビット数の乱数である”bbbbbbbb”の値を有するバージョン2である配送用鍵Kdは、1998年2月1日から1998年2月28日まで使用可能（すなわち、その期間にサービスプロバイダ3を介してユーザホームネットワーク5に配布されるコンテンツを暗号化するコンテンツ鍵Kcoは、バージョン2である配送用鍵Kdで暗号化されている）である。同様に、バージョン3である配送用鍵Kdは、1998年3月中に使用可能であり、バージョン4である配送用鍵Kdは、1998年4月中に使用可能であり、バージョン5である配送用鍵Kdは、1998年5月中に使用可能であり、バージョン6である配送用鍵Kdは、1998年6月中に使用可能である。

## 【0034】

コンテンツプロバイダ2がコンテンツの提供を開始するに先立ち、EMDサービスセンタ1は、コンテンツプロバイダ2に、1998年1月から1998年6月まで利用可能な、バージョン1乃至バージョン6の6つの配送用鍵Kdを送信し、コンテンツプロバイダ2は、6つの配送用鍵Kdを受信し、記憶する。6月分の配送用鍵Kdを記憶するのは、コンテンツプロバイダ2が、コンテンツを提供

する前のコンテンツおよびコンテンツ鍵の暗号化などの準備に、所定の期間が必要だからである。

【0035】

また、レシーバ51がコンテンツの利用を開始するに先立ち、EMDサービスセンタ1は、レシーバ51に、1998年1月から1998年3月まで、利用可能なバージョン1乃至バージョン3である3つの配送用鍵Kdを送信し、レシーバ51は、3つの配送用鍵Kdを受信し、記憶する。3月分の配送用鍵Kdを記憶するのは、レシーバ51が、EMDサービスセンタ1に接続できないなどのトラブルにより、コンテンツの利用が可能な契約期間にもかかわらずコンテンツが利用できない等の事態を避けるためであり、また、EMDサービスセンタ1への接続の頻度を低くし、ユーザホームネットワーク5の負荷を低減するためである。

【0036】

1998年1月1日から1998年1月31日の期間には、バージョン1である配送用鍵Kdが、EMDサービスセンタ1、コンテンツプロバイダ2、ユーザホームネットワーク5を構成するレシーバ51で利用される。

【0037】

1998年2月1日における、EMDサービスセンタ1の配送用鍵Kdのコンテンツプロバイダ2、およびレシーバ51への送信を図5で説明する。EMDサービスセンタ1は、コンテンツプロバイダ2に、1998年2月から1998年7月まで利用可能な、バージョン2乃至バージョン7の6つの配送用鍵Kdを送信し、コンテンツプロバイダ2は、6つの配送用鍵Kdを受信し、受信前に記憶していた配送用鍵Kdに上書きし、新たな配送用鍵Kdを記憶する。EMDサービスセンタ1は、レシーバ51に、1998年2月から1998年4月まで、利用可能なバージョン2乃至バージョン4である3つの配送用鍵Kdを送信し、レシーバ51は、3つの配送用鍵Kdを受信し、受信前に記憶していた配送用鍵Kdに上書きし、新たな配送用鍵Kdを記憶する。EMDサービスセンタ1は、バージョン1である配送用鍵Kdをそのまま記憶する。これは、不測のトラブルが発生したとき、若しくは不正が発生し、または発見されたときに、過去に利用した配送用鍵Kdを利用できるようにするためである。

## 【0038】

1998年2月1日から1998年2月28日の期間には、バージョン2である配送用鍵K dが、EMDサービスセンタ1、コンテンツプロバイダ2、ユーザホームネットワーク5を構成するレシーバ51で利用される。

## 【0039】

1998年3月1日における、EMDサービスセンタ1の配送用鍵K dのコンテンツプロバイダ2、およびレシーバ51への送信を図6で説明する。EMDサービスセンタ1は、コンテンツプロバイダ2に、1998年3月から1998年8月まで利用可能な、バージョン3乃至バージョン8の6つの配送用鍵K dを送信し、コンテンツプロバイダ2は、6つの配送用鍵K dを受信し、受信前に記憶していた配送用鍵K dに上書きし、新たな配送用鍵K dを記憶する。EMDサービスセンタ1は、レシーバ51に、1998年3月から1998年5月まで、利用可能なバージョン3乃至バージョン5である3つの配送用鍵K dを送信し、レシーバ51は、3つの配送用鍵K dを受信し、受信前に記憶していた配送用鍵K dに上書きし、新たな配送用鍵K dを記憶する。EMDサービスセンタ1は、バージョン1である配送用鍵K dおよびバージョン2である配送用鍵K dをそのまま記憶する。

## 【0040】

1998年3月1日から1998年3月31日の期間には、バージョン3である配送用鍵K dが、EMDサービスセンタ1、コンテンツプロバイダ2、ユーザホームネットワーク5を構成するレシーバ51で利用される。

## 【0041】

1998年4月1日における、EMDサービスセンタ1の配送用鍵K dのコンテンツプロバイダ2、およびレシーバ51への送信を図7で説明する。EMDサービスセンタ1は、コンテンツプロバイダ2に、1998年4月から1998年9月まで利用可能な、バージョン4乃至バージョン9の6つの配送用鍵K dを送信し、コンテンツプロバイダ2は、6つの配送用鍵K dを受信し、受信前に記憶していた配送用鍵K dに上書きし、新たな配送用鍵K dを記憶する。EMDサービスセンタ1は、レシーバ51に、1998年4月から1998年6月まで、利用可能

なバージョン3乃至バージョン5である3つの配送用鍵K dを送信し、レシーバ51は、3つの配送用鍵K dを受信し、受信前に記憶していた配送用鍵K dに上書きし、新たな配送用鍵K dを記憶する。EMDサービスセンタ1は、バージョン1である配送用鍵K d、バージョン2である配送用鍵K d、およびバージョン3である配送用鍵K dをそのまま記憶する。

【0042】

1998年4月1日から1998年4月30日の期間には、バージョン4である配送用鍵K dが、EMDサービスセンタ1、コンテンツプロバイダ2、ユーザホームネットワーク5を構成するレシーバ51で利用される。

【0043】

このように、あらかじめ先の月の配送用鍵K dを配布しておくことで、仮にユーザが1、2ヶ月まったくEMDサービスセンタ1にアクセスしていなくても、一応、コンテンツの買い取りが行え、時を見計らって、EMDサービスセンタ1にアクセスして鍵を受信することができる。

【0044】

図3に戻り、経歴データ管理部15は、ユーザ管理部18から出力される、課金情報、そのコンテンツに対応するPT、およびそのコンテンツに対応するUCPなどを記憶する。

【0045】

利益分配部16は、経歴データ管理部15から供給された各種情報に基づき、EMDサービスセンタ1、コンテンツプロバイダ2、およびサービスプロバイダ3の利益をそれぞれ算出し、その結果をサービスプロバイダ管理部11、コンテンツプロバイダ管理部12、出納部20、および著作権管理部13に出力する。

【0046】

相互認証部17は、コンテンツプロバイダ2、サービスプロバイダ3、およびユーザホームネットワーク5の機器と相互認証を実行する。

【0047】

ユーザ管理部18は、EMDシステムに登録可能な、ユーザホームネットワーク5の機器に関する情報（以下、システム登録情報と称する）を管理する。システ

ム登録情報には、図8に示すように、「SAMのID」、「機器番号」、「決済ID」、「決済ユーザ情報」、複数の「従属ユーザ情報」、および「利用ポイント情報」の項目に対応する情報が含まれる。

【0048】

「SAMのID」には、製造された、ユーザホームネットワーク5の機器のSAMのIDが記憶される。図8のシステム登録情報の「SAMのID」には、レシーバ51のSAM62のID、レシーバ201のSAM212のID、およびレシーバ301のSAM311のIDが設定されている。

【0049】

「機器番号」には、SAMを有するユーザホームネットワーク5の機器に、予め設定された機器番号が設定されている。ユーザホームネットワーク5の機器が、ネットワーク4を介してサービスプロバイダ3と、およびEMDサービスセンタ1と直接通信することができる機能を有し（通信部を有し）、かつ、例えば、UCPやPTの内容をユーザに出力（提示）したり、ユーザがUCPの利用内容を選択することができる機能を有している（表示部および操作部を有している）場合、その機器（以下、このような機能を有する機器を主機器と称する）には、100番以上の機器番号が与えられる。機器が、そのような機能を有しない場合、その機器（以下、このような機器を従機器と称する）には、99番以下の機器番号が与えられる。この例の場合、詳細は後述するが、レシーバ51およびレシーバ201の両者は、上述した機能を有しているので、主機器とされ、対応する「機器番号」には、機器番号100番がそれぞれ設定されている。一方、レシーバ301は、上述した機能を有していないので、従機器とされ、対応する「機器番号」には、機器番号25番が設定されている。

【0050】

「決済ID」には、課金を決済するユーザ（以下、決済ユーザと称する）に割り当てられた所定の決済IDが設定される。この例の場合、レシーバ51、レシーバ201、およびレシーバ301は、ユーザFが決済ユーザとされて登録されているので、それらの「決済ID」には、ユーザFの決済IDが、それぞれ設定されている。

## 【0051】

「決済ユーザ情報」には、決済ユーザの、氏名、住所、電話番号、決済機関情報（例えば、クレジットカード番号等）、生年月日、年齢、性別、ID、パスワードなどが設定される。「決済ユーザ情報」に設定される決済ユーザの、氏名、住所、電話番号、決済機関の情報、生年月日、年齢、および性別（以下、「決済ユーザ情報」に設定されるこれらの情報を、個々に区別する必要がない場合、まとめて、ユーザー一般情報と称する）は、登録が申請される際にユーザから提供され、設定される。また、この例の場合、そのうちの、氏名、住所、電話番号、および決済機関の情報は、それらに基づいて与信処理が行われるので、正確な情報（例えば、決済機関に登録されている情報）である必要がある。それに対してユーザー一般情報の生年月日、年齢、および性別は、与信処理には用いられないので、この例の場合、それらの情報は、正確である必要はなく、またユーザは、その情報を必ずしも提供する必要がない。「決済ユーザ情報」に記憶される決済ユーザの、IDおよびパスワードは、EMDシステムに登録されるときに割り当てられ、設定される。

## 【0052】

図8のシステム登録情報の、レシーバ51のSAM62のID、レシーバ201のSAM212のID、およびレシーバ301のSAM311のIDに対応する「決済ユーザ情報」には、ユーザFから提供されたユーザー一般情報、ユーザFのID、およびユーザFのパスワードが設定されている。

## 【0053】

「従属ユーザ情報」には、課金を決済しないユーザ（以下、このようなユーザを従属ユーザと称する）の、氏名、住所、電話番号、生年月日、年齢、性別、ID、パスワードなどが設定される。すなわち、「決済ユーザ情報」に設定される情報のうち、決済機関の情報以外の情報が設定される。

## 【0054】

従属ユーザに対しては与信処理が行われないので、「従属ユーザ情報」に設定される従属ユーザの、氏名、住所、電話番号、生年月日、年齢、および性別の情報は、正確なものである必要がない。例えば、氏名の場合は、ニックネームのよ

うなものでもよい。また氏名はユーザを特定するために必要とされるが、他の情報は、ユーザは必ずしも提供する必要がない。「従属ユーザ情報」に設定される従属ユーザの、IDおよびパスワードは、登録されるときに割り当てられ、設定される。

#### 【0055】

この例の場合、レシーバ201およびレシーバ301の両者には、ユーザAが、従属ユーザとして登録されていないので、図8のシステム登録情報の、レシーバ201のSAM212のIDおよびレシーバ301のSAM311のIDに対応する「従属ユーザ情報」には、ユーザAから提供されたユーザ一般情報（決済機関情報を除く）、ユーザAのID、およびユーザAのパスワードが設定されている。レシーバ51には、従属ユーザが設けられていないので、SAM62のIDに対応する「従属ユーザ情報」には、何の情報も設定されていない。

#### 【0056】

「利用ポイント情報」には、利益分配部16から出力された利用ポイントが設定される。図8のシステム登録情報の、レシーバ51のSAM62のID、レシーバ201のSAM212のID、およびレシーバ301のSAM311のIDに対応する「利用ポイント情報」には、それぞれの利用ポイント情報が設定されている。

#### 【0057】

ユーザ管理部18は、このようなシステム登録情報を管理する他、所定の処理に対応して登録リスト（後述）を作成し、配送用鍵Kdとともにユーザホームネットワーク5に送信する。

#### 【0058】

課金請求部19は、経歴データ管理部15から供給された、例えば、課金情報、UCP、およびPTに基づき、ユーザへの課金を算出し、その結果を、出納部20に供給する。出納部20は、ユーザ、コンテンツプロバイダ2、およびサービスプロバイダ3への出金、徴収すべき利用料金の金額を基に、図示せぬ外部の銀行等と通信し、決算処理を実行する。出納部20はまた、決算処理の結果をユーザ管理部18に通知する。監査部21は、ユーザホームネットワーク5の機器から供給された課金情報、PT、およびUCPの正当性（すなわち、不正をしていないか

)を監査する。

【0059】

図9は、コンテンツプロバイダ2の機能的構成を示すブロック図である。コンテンツサーバ31は、ユーザに供給するコンテンツを記憶し、ウォーターマーク付加部32に供給する。ウォーターマーク付加部32は、コンテンツサーバ31から供給されたコンテンツにウォーターマーク（電子透かし）を付加し、圧縮部33に供給する。

【0060】

圧縮部33は、ウォーターマーク付加部32から供給されたコンテンツを、ATRA C2(Adaptive Transform Acoustic Coding 2)（商標）等の方式で圧縮し、暗号化部34に供給する。暗号化部34は、圧縮部33で圧縮されたコンテンツを、乱数発生部35から供給された乱数を鍵（以下、この乱数をコンテンツ鍵 $K_c$ と称する）として、DES(Data Encryption Standard)などの共通鍵暗号方式で暗号化し、その結果をセキュアコンテナ作成部38に出力する。

【0061】

乱数発生部35は、コンテンツ鍵 $K_c$ となる所定のビット数の乱数を暗号化部34および暗号化部36に供給する。暗号化部36は、コンテンツ鍵 $K_c$ をEMDサービスセンタ1から供給された配送用鍵 $K_d$ を使用して、DESなどの共通鍵暗号方式で暗号化し、その結果をセキュアコンテナ作成部38に出力する。

【0062】

DESは、56ビットの共通鍵を用い、平文の64ビットを1ブロックとして処理する暗号方式である。DESの処理は、平文を攪拌し、暗号文に変換する部分（データ攪拌部）と、データ攪拌部で使用する鍵（拡大鍵）を共通鍵から生成する部分（鍵処理部）からなる。DESのすべてのアルゴリズムは公開されているので、ここでは、データ攪拌部の基本的な処理を簡単に説明する。

【0063】

まず、平文の64ビットは、上位32ビットの $H_0$ 、および下位32ビットの $L_0$ に分割される。鍵処理部から供給された48ビットの拡大鍵 $K_1$ 、および下位32ビットの $L_0$ を入力とし、下位32ビットの $L_0$ を攪拌したF関数の出力が算



出される。F関数は、数値を所定の規則で置き換える「換字」およびビット位置を所定の規則で入れ替える「転置」の2種類の基本変換から構成されている。次に、上位32ビットの $H_0$ と、F関数の出力が排他的論理和され、その結果は $L_1$ とされる。 $L_0$ は、 $H_1$ とされる。

## 【0064】

上位32ビットの $H_0$ および下位32ビットの $L_0$ を基に、以上の処理を16回繰り返し、得られた上位32ビットの $H_{16}$ および下位32ビットの $L_{16}$ が暗号文として出力される。復号は、暗号化に使用した共通鍵を用いて、上記の手順を逆にたどることで実現される。

## 【0065】

ポリシー記憶部37は、コンテンツに対応して設定されるUCPを記憶し、セキュアコンテナ作成部38に出力する。図10は、コンテンツサーバ31に保持されているコンテンツAに対応して設定され、ポリシー記憶部37に記憶されているUCPAを表している。UCPには、「コンテンツのID」、「コンテンツプロバイダのID」、「UCPのID」、「UCPの有効期限」、「利用条件」、および「利用内容」の各項目に対応する所定の情報が含まれる。「コンテンツのID」には、UCPが対応するコンテンツのIDが設定される。UCPAの「コンテンツのID」には、コンテンツAのIDが設定されている。

## 【0066】

「コンテンツプロバイダのID」には、コンテンツの提供元のコンテンツプロバイダのIDが設定され、UCPAの「コンテンツプロバイダのID」には、コンテンツプロバイダ2のIDが設定されている。「UCPのID」には、各UCPに割り当てられた所定のIDが設定され、UCPAの「UCPのID」には、UCPAのIDが設定されている。

「UCPの有効期限」には、UCPの有効期限を示す情報が設定され、UCPAの「UCPの有効期限」には、UCPAの有効期限が設定されている。

## 【0067】

「利用条件」には、「ユーザ条件」および「機器条件」の各項目に対応する所定の情報が設定される。「ユーザ条件」には、このUCPを選択することができるユーザの条件が設定され、「機器条件」には、このUCPを選択することができる

機器の条件が設定される。

【0068】

UCPAの場合、「利用条件10」が設定され、「利用条件10」の「ユーザ条件10」には、EMDシステムの利用頻度などに対応して与えられる所定の利用ポイントが200ポイント以上であることを示す情報（“200ポイント以上”）が設定されている。また「利用条件10」の「機器条件10」には、条件がないことを示す情報（“条件なし”）が設定されている。すなわち、UCPAは、200ポイント以上の利用ポイントを有するユーザのみが選択可能となる。

【0069】

「利用内容」には、「ID」、「形式」、「パラメータ」、および「管理移動許可情報」の各項目に対応する所定の情報が含まれる。「ID」には、「利用内容」に設定される情報に割り当てられた所定のIDが設定される。「形式」には、再生や複製など、コンテンツの利用形式を示す情報が設定される。「パラメータ」には、「形式」に設定された利用形式に対応する所定の情報が設定される。

【0070】

「管理移動許可情報」には、コンテンツの管理移動が可能か否か（許可されているか否か）を示す情報が設定される。コンテンツの管理移動が行われると、図11（A）に示すように、管理移動元の機器にコンテンツが保持されつつ、管理移動先の機器にそのコンテンツが移動される。すなわち、管理移動元の機器と管理移動先の機器の両方において、コンテンツが利用される。この点で、図11（B）に示すように、移動元の機器にコンテンツが保持されず、移動先の機器のみにコンテンツが保持され、移動先の機器においてのみコンテンツが利用される、通常の移動とは異なる。

【0071】

また、コンテンツの管理移動が行われている間、管理移動元の機器は、図11（A）に示すように、他の機器にコンテンツを管理移動することができない（許可されない）。すなわち、管理移動元の機器と管理移動先の機器の2機においてのみコンテンツが保持される。この点で、図12（A）に示すように、オリジナルのコンテンツから、複数の複製（第1世代）を作成することができる、第1世

代の複製とも異なる。また、管理移動元の機器からコンテンツを戻すことより、他の機器にコンテンツを管理移動することができるので、この点で、図 12 (B) に示すように、1 回だけの複製とも異なる。

#### 【0072】

図 10 に戻り、UCPA には、6 つの「利用内容 1 1」乃至「利用内容 1 6」が設けられており、「利用内容 1 1」において、その「ID 1 1」には、「利用内容 1 1」に割り当てられた所定の ID が設定されている。「形式 1 1」には、コンテンツを買い取って再生する利用形式を示す情報（” 買い取り再生”）が設定される。ユーザは、” 買い取り再生” の利用形式で利用する権利を購入することより、コンテンツ A を制限なしに再生することができる。「パラメータ 1 1」には、” 買い取り再生” に対応する所定の情報が設定されている。「管理移動許可情報 1 1」には、コンテンツの管理移動が許可されていることを示す情報（” 可”）が設定されている。

#### 【0073】

「利用内容 1 2」において、その「ID 1 2」には、「利用内容 1 2」に割り当てられた所定の ID が設定されている。「形式 1 2」には、第 1 世代の複製を行う利用形式を示す情報（” 第 1 世代複製”）が設定されている。ユーザは、” 第 1 世代複製” の利用形式で利用する権利を購入することより、図 12 (A) に示したように、オリジナルのコンテンツ A から、複数の第 1 世代の複製を作成することができる。なお、この場合、第 1 世代の複製から第 2 世代の複製を作成することはできない（許可されない）。「パラメータ 1 2」には、” 第 1 世代複製” に対応する所定の情報が設定されている。「管理移動許可情報 1 2」には、コンテンツの管理移動が許可されていないことを示す情報（” 不可”）が設定されている。

#### 【0074】

「利用内容 1 3」において、その「ID 1 3」には、「利用内容 1 3」に割り当てられた所定の ID が設定されている。「形式 1 3」には、” 期間制限再生” の利用形式が設定されている。ユーザは、” 期間制限再生” の利用形式で利用する権利を購入することより、所定の期間（時間）に限ってコンテンツ A を再生するこ

とができる。「パラメータ13」には、「期間制限再生」に対応して、その期間の開始時期（時刻）と終了時期（時刻）が設定されている。「管理移動許可情報13」には、「可」が設定されている。

#### 【0075】

「利用内容14」において、その「ID14」には、「利用内容14」に割り当てられた所定のIDが設定されている。「形式14」には、「Pay Per CopyN」の利用形式が設定されている。ユーザは、「Pay Per CopyN」の利用形式で利用する権利を購入することより、オリジナルのコンテンツAから、N個の複製を作成することができる（許可される）。なお、「Pay Per CopyN」の場合も、図12の（B）に示すように、複製からの複製を作成することはできない（許可されない）。「パラメータ14」には、「Pay Per CopyN」に対応する所定の情報が設定されている。「管理移動許可情報14」には、「不可」が設定されている。

#### 【0076】

「利用内容15」において、その「ID15」には、「利用内容15」に割り当てられた所定のIDが設定されている。「形式15」には、「形式13→形式11」の利用形式が設定されている。ユーザは、「期限制限再生」の利用形式で利用する権利をすでに購入しているとき、この利用形式で利用する権利を購入することができ、それにより、ユーザは、コンテンツAを「買い取り再生」（形式11）で利用することができる。「パラメータ15」には、「形式13→形式11」に対応する所定の情報が設定されている。「管理移動許可情報15」には、「可」が設定されている。

#### 【0077】

「利用内容16」において、その「ID16」には、「利用内容16」に割り当てられた所定のIDが設定されている。「形式16」には、「形式11→形式11」の利用形式が設定されている。ユーザは、「買い取り再生」（形式11）の利用形式で利用する権利をすでに購入しているとき、この利用形式で利用する権利を購入することができ、それにより、ユーザは、再度、コンテンツAを「買い取り再生」で利用することができる。この利用形式で利用する権利は、例えば、レシーバ51において「買い取り再生」で利用する権利が購入され、コンテンツ

Aが利用されているとき、レシーバ301またはレシーバ201において、コンテンツAを”買い取り再生”で利用したい場合に購入される。「パラメータ16」には、”形式11-形式11”に対応する所定の情報が設定されている。「管理移動許可情報16」には、”可”が設定されている。

## 【0078】

図9に戻り、セキュアコンテナ作成部38は、例えば、図13に示すような、コンテンツA（コンテンツ鍵KcoAで暗号化されている）、コンテンツ鍵KcoA（配送用鍵Kdで暗号化されている）、UCPA、およびその署名からなるコンテンツプロバイダセキュアコンテナを作成する。なお、署名は、送信したいデータ（この場合、コンテンツA（コンテンツ鍵KcoAで暗号化されている））、コンテンツ鍵KcoA（配送用鍵Kdで暗号化されている）、およびUCPAの全体にハッシュ関数を適用して得られたハッシュ値が、公開鍵暗号の秘密鍵（この場合、コンテンツプロバイダ2の秘密鍵Kscp）で暗号化されたものである。

## 【0079】

セキュアコンテナ作成部38はまた、コンテンツプロバイダセキュアコンテナに、図14に示すコンテンツプロバイダ2の証明書を付してサービスプロバイダ3に送信する。この証明書は、証明書のバージョン番号、認証局がコンテンツプロバイダ2に対し割り付けた証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、およびコンテンツプロバイダ2の名前、コンテンツプロバイダ2の公開鍵Kpcp、並びにその署名（認証局の秘密鍵Kscaで暗号化されている）から構成されている。

## 【0080】

署名は、改竄のチェックおよび作成者認証をするためのデータであり、送信したいデータを基にハッシュ関数でハッシュ値をとり、これを公開鍵暗号の秘密鍵で暗号化して作成される。

## 【0081】

ハッシュ関数および署名の照合について説明する。ハッシュ関数は、送信したい所定のデータを入力とし、所定のビット長のデータに圧縮し、ハッシュ値とし

て出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの1ビットが変化するとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ入力データを探し出すことが困難である特徴を有する。

#### 【0082】

署名とデータを受信した受信者は、署名を公開鍵暗号の公開鍵で復号し、その結果（ハッシュ値）を得る。さらに受信されたデータのハッシュ値が計算され、計算されたハッシュ値と、署名を復号して得られたハッシュ値とが、等しいか否かが判定される。送信されたデータのハッシュ値と復号したハッシュ値が等しいと判定された場合、受信したデータは改竄されておらず、公開鍵に対応した秘密鍵を保持する送信者から送信されたデータであることがわかる。署名のハッシュ関数としては、MD4、MD5、SHA-1などが用いられる。

#### 【0083】

次に公開鍵暗号について説明する。暗号化および復号で同一の鍵（共通鍵）を使用する共通鍵暗号方式に対し、公開鍵暗号方式は、暗号化に使用する鍵と復号するときの鍵が異なる。公開鍵暗号を用いる場合、鍵の一方を公開しても他方を秘密に保つことができ、公開しても良い鍵は、公開鍵と称され、他方の秘密に保つ鍵は、秘密鍵と称される。

#### 【0084】

公開鍵暗号の中で代表的なRSA（Rivest-Shamir-Adleman）暗号を、簡単に説明する。まず、2つの十分に大きな素数である $p$ および $q$ を求め、さらに $p$ と $q$ の積である $n$ を求める。 $(p-1)$ と $(q-1)$ の最小公倍数 $L$ を算出し、更に、3以上 $L$ 未満で、かつ、 $L$ と互いに素な数 $e$ を求める（すなわち、 $e$ と $L$ を共通に割り切れる数は、1のみである）。

#### 【0085】

次に、 $L$ を法とする乗算に関する $e$ の乗法逆元 $d$ を求める。すなわち、 $d$ 、 $e$ 、および $L$ の間には、 $ed=1 \bmod L$ が成立し、 $d$ はユークリッドの互除法で算出できる。このとき、 $n$ と $e$ が公開鍵とされ、 $p$ 、 $q$ 、および $d$ が、秘密鍵とされる。

#### 【0086】

暗号文Cは、平文Mから、式(1)の処理で算出される。

【0087】

$$C = M^e \bmod n \quad (1)$$

暗号文Cは、式(2)の処理で平文Mに、復号される。

【0088】

$$M = C^d \bmod n \quad (2)$$

証明は省略するが、RSA暗号で平文を暗号文に変換して、それが復号できるのは、フェルマーの小定理に根拠をおいており、式(3)が成立するからである。

【0089】

$$M = C^d = (M^e)^d = M^{ed} = M \bmod n \quad (3)$$

秘密鍵pとqを知っているならば、公開鍵eから秘密鍵dは算出できるが、公開鍵nの素因数分解が計算量的に困難な程度に公開鍵nの桁数を大きくすれば、公開鍵nを知るだけでは、公開鍵eから秘密鍵dは計算できず、復号できない。以上のように、RSA暗号では、暗号化に使用する鍵と復号するときの鍵を、異なる鍵とすることができる。

【0090】

また、公開鍵暗号の他の例である楕円曲線暗号についても、簡単に説明する。楕円曲線 $y^2 = x^3 + ax + b$ 上の、ある点をBとする。楕円曲線上の点の加算を定義し、 $nB$ は、Bをn回加算した結果を表す。同様に、減算も定義する。Bと $nB$ からnを算出することは、困難であることが証明されている。Bと $nB$ を公開鍵とし、nを秘密鍵とする。乱数rを用いて、暗号文C1およびC2は、平文Mから、公開鍵で式(4)および式(5)の処理で算出される。

【0091】

$$C1 = M + rnB \quad (4)$$

$$C2 = rB \quad (5)$$

暗号文C1およびC2は、式(6)の処理で平文Mに、復号される。

【0092】

$$M = C1 - nC2 \quad (6)$$

復号できるのは、秘密鍵nを有するものだけである。以上のように、RSA暗号と

同様に、楕円曲線暗号でも、暗号化に使用する鍵と復号するときの鍵を、異なる鍵とすることができる。

#### 【0093】

図9に再び戻り、コンテンツプロバイダ2の相互認証部39は、EMDサービスセンタ1から配送用鍵Kdの供給を受けるのに先立ち、EMDサービスセンタ1と相互認証する。また相互認証部39は、サービスプロバイダ3へのコンテンツプロバイダセキュアコンテナの送信に先立ち、サービスプロバイダ3と相互認証することも可能であるが、この例の場合、コンテンツプロバイダセキュアコンテナには、秘密にしなければならない情報が含まれていないので、この相互認証は、必ずしも必要とされない。

#### 【0094】

次に、図15のブロック図を参照して、サービスプロバイダ3の機能的構成を説明する。コンテンツサーバ41は、コンテンツプロバイダ2から供給されたコンテンツプロバイダセキュアコンテナに含まれる、コンテンツ（コンテンツ鍵Kcoで暗号化されている）、コンテンツ鍵Kco（配送用鍵Kdで暗号化されている）、UCP、およびコンテンツプロバイダ2の署名を記憶し、セキュアコンテナ作成部44に供給する。

#### 【0095】

値付け部42は、コンテンツプロバイダ2から供給されたコンテンツプロバイダセキュアコンテナに含まれる署名に基づいて、コンテンツプロバイダセキュアコンテナの正当性を検証し、その正当性を確認すると、コンテンツプロバイダセキュアコンテナに含まれるUCPに対応する、PTを作成し、セキュアコンテナ作成部44に供給する。図16は、図10のUCPAに対応して作成された、2つのPTA-1（図16（A））およびPTA-2（図16（B））を表している。PTには、「コンテンツのID」、「コンテンツプロバイダのID」、「UCPのID」、「サービスプロバイダのID」、「PTのID」、「PTの有効期限」、「価格条件」、および「価格内容」の各項目に設定される所定の情報が含まれる。

#### 【0096】

PTの、「コンテンツのID」、「コンテンツプロバイダのID」、および「UCPのI



D」の各項目には、UCPの、これらに対応する項目の情報が、それぞれ設定される。すなわち、PTA-1およびPTA-2のそれぞれの「コンテンツのID」には、コンテンツAのIDが、それぞれの「コンテンツプロバイダのID」には、コンテンツプロバイダ2のIDが、そしてそれぞれの「UCPのID」には、UCPAのIDが設定されている。

## 【0097】

「サービスプロバイダのID」には、PTの提供元のサービスプロバイダ3のIDが設定される。PTA-1およびPTA-2のそれぞれの「サービスプロバイダのID」には、サービスプロバイダ3のIDが設定されている。「PTのID」には、各PTに割り当てられた所定のIDが設定され、PTA-1の「PTのID」には、PTA-1のIDが、PTA-2の「PTのID」には、PTA-2のIDがそれぞれ設定されている。「PTの有効期限」には、PTの有効期限を示す情報が設定され、PTA-1の「PTの有効期限」には、PTA-1の有効期限が、PTA-2の「PTの有効期限」には、PTA-2の有効期限が設定されている。

## 【0098】

「価格条件」は、UCPの「利用条件」と同様に、「ユーザ条件」および「機器条件」の項目からなり、その「ユーザ条件」には、このPTを選択することができるユーザの条件を示す情報が設定され、その「機器条件」には、このPTを選択することができる機器の条件を示す情報が設定される。

## 【0099】

PTA-1の場合、「価格条件10」が設定され、「価格条件10」の「ユーザ条件10」には、ユーザが男性であることを示す情報（”男性”）が設定され、その「機器条件10」には、”条件なし”が設定されている。すなわち、PTA-1は、男性のユーザのみが選択可能となる。

## 【0100】

PTA-2の場合、「価格条件20」が設定され、「価格条件20」の「ユーザ条件20」には、ユーザが女性であることを示す情報（”女性”）が設定され、その「機器条件20」には、”条件なし”が設定されている。すなわち、PTA-2は、女性のユーザのみが選択可能となる。

## 【0101】

PTの「価格内容」には、対応するUCPの「利用内容」の「形式」に設定されている利用形式の利用料金（利用形式でコンテンツを利用する権利の価格）が示されている。PTA-1の「価格内容11」の”2000円”とPTA-2の「価格内容21」の”1000円”は、コンテンツAを”買い取り再生”の利用形式で利用する場合の料金（”買い取り再生”の利用形式で利用する権利の価格）を示している。

## 【0102】

PTA-1の「価格内容12」の”600円”およびPTA-2の「価格内容22」の”300円”は、UCPAの「利用内容12」の「形式12」より、”第1世代複製”の利用形式でコンテンツAを利用する権利の価格を示している。PTA-1の「価格内容13」の”100円”およびPTA-2の「価格内容23」の”50円”は、UCPAの「利用内容13」の「形式13」より、”期間制限再生”の利用形式でコンテンツAを利用する権利の価格を示している。PTA-1の「価格内容14」の”300円”およびPTA-2の「価格内容24」の”150円”は、UCPAの「利用内容14」の「形式14」より、”Pay Per CopyN”の利用形式でコンテンツAを利用する権利の価格を示している。

## 【0103】

PTA-1の「価格内容15」の”1950円”およびPTA-2の「価格内容25」の”1980円”は、UCPAの「利用内容15」の「形式15」より、”期間制限再生”の権利を有しているときの、”買い取り再生”の権利の価格を示している。PTA-1の「価格内容16」の”1000円”およびPTA-2の「価格内容26」の”500円”は、UCPAの「利用内容16」の「形式16」より、”買い取り再生”の権利を有しているときの、”買い取り再生”の権利の価格を示している。

## 【0104】

なお、この例の場合、PTA-1（男性ユーザに適用される）の価格内容と、PTA-2（女性ユーザに適用される）の価格内容を比較すると、PTA-1の価格内容に示される価格が、PTA-2の価格内容に示される価格の2倍に設定されてい

る。例えば、UCPAの「利用内容11」に対応するPTA-1の「価格内容11」が”2000円”とされているのに対し、同様にUCPAの「利用内容11」に対応するPTA-2の「価格内容21」は”1000円”とされている。同様、PTA-1の「価格内容12」乃至「価格内容14」に設定されている価格は、PTA-2の「価格内容22」乃至「価格内容24」に設定されている価格の2倍とされている。すなわち、コンテンツAは、女性ユーザがより低価格で利用することができるコンテンツである。

## 【0105】

図15に戻り、ポリシー記憶部43は、コンテンツプロバイダ2から供給された、コンテンツのUCPを記憶し、セキュアコンテナ作成部44に供給する。

## 【0106】

セキュアコンテナ作成部44は、例えば、図17に示すような、コンテンツA（コンテンツ鍵KcoAで暗号化されている）、コンテンツ鍵KcoA（配送用鍵Kdで暗号化されている）、UCPA、コンテンツプロバイダ2の署名、PTA-1、A-2、およびサービスプロバイダ3の署名からなるサービスプロバイダセキュアコンテナを作成する。

## 【0107】

セキュアコンテナ作成部44はまた、作成したサービスプロバイダセキュアコンテナを、図18に示すような、証明書のバージョン番号、認証局がサービスプロバイダ3に対し割り付ける証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、サービスプロバイダ3の名前、サービスプロバイダ3の公開鍵Kpsp、並びに署名より構成されるサービスプロバイダの証明書を付して、ユーザホームネットワーク5に供給する。

## 【0108】

図15に、再び戻り、相互認証部45は、コンテンツプロバイダ2からコンテンツプロバイダセキュアコンテナの供給を受け取るのに先立ち、コンテンツプロバイダ2と相互認証する。相互認証部45また、ユーザホームネットワーク5へのサービスプロバイダセキュアコンテナの送信に先立ち、ユーザホームネットワーク5と相互認証するが、このサービスプロバイダ3とユーザホームネットワー

ク 5 との相互認証は、例えば、ネットワーク 4 が衛星通信である場合、実行されない。なお、この例の場合、コンテンツプロバイダセキュアコンテナおよびサービスプロバイダセキュアコンテナには、特に、秘密情報が含まれていないので、サービスプロバイダ 3 は、コンテンツプロバイダ 2 およびユーザホームネットワーク 5 と相互認証を行わなくてもよい。

#### 【0109】

図 19 は、ユーザホームネットワーク 5 を構成するレシーバ 51 の構成例を表している。レシーバ 51 は、通信部 61、SAM 62、外部記憶部 63、伸張部 64、通信部 65、インタフェース 66、表示制御部 67、および入力制御部 68 より構成される据え置き型の機器である。

#### 【0110】

レシーバ 51 の通信部 61 は、ネットワーク 4 を介してサービスプロバイダ 3、または EMD サービスセンタ 1 と通信し、所定の情報を受信し、または送信する。

#### 【0111】

SAM 62 は、相互認証モジュール 71、課金処理モジュール 72、記憶モジュール 73、復号／暗号化モジュール 74、およびデータ検査モジュール 75 になるが、シングルチップの暗号処理専用 IC で構成され、多層構造を有し、その内部のメモリセルはアルミニウム層等のダミー層に挟まれ、また、動作する電圧または周波数の幅が狭い等、外部から不正にデータが読み出し難い特性（耐タンパー性）を有している。

#### 【0112】

SAM 62 の相互認証モジュール 71 は、記憶モジュール 73 に記憶されている、図 20 に示す SAM 62 の証明書を、相互認証相手に送信し、相互認証を実行し、これにより、認証相手と共有することとなった一時鍵  $K_{temp}$ （セッション鍵）を復号／暗号化モジュール 74 に供給する。SAM の証明書には、コンテンツプロバイダ 2 の証明書（図 14）およびサービスプロバイダ 3 の証明書（図 18）に含まれている情報に対応する情報が含まれているので、その説明は省略する。

## 【0113】

課金処理モジュール72は、選択されたUCPの利用内容に基づいて、UCSおよび課金情報を作成する。図21は、図10に示したUCPAの利用内容13と、図16(A)に示したPTA-1の「価格内容13」に基づいてAを表している。UCSには、図21に示されるように、「コンテンツのID」、「コンテンツプロバイダのID」、「UCPのID」、「UCPの有効期限」、「サービスプロバイダのID」、「PTのID」、「PTの有効期限」、「UCSのID」、「SAMのID」、「ユーザのID」、「利用内容」、および「利用履歴」の各項目に設定される情報が含まれている。

## 【0114】

UCSの、「コンテンツのID」、「コンテンツプロバイダのID」、「UCPのID」、「UCPの有効期限」、「サービスプロバイダのID」、「PTのID」、および「PTの有効期限」の各項目には、PTの、それらに対応する項目の情報が設定される。すなわち、図21のUCSAの、「コンテンツのID」には、コンテンツAのIDが、「コンテンツプロバイダのID」には、コンテンツプロバイダ2のIDが、「UCPのID」には、UCPAのIDが、「UCPの有効期限」には、UCPAの有効期限が、「サービスプロバイダのID」には、サービスプロバイダ3のIDが、「PTのID」には、PTA-1のIDが、そして「PTの有効期限」には、PTA-1の有効期限が、それぞれ設定されている。

## 【0115】

「UCSのID」には、UCSに割り当てられた所定のIDが設定され、UCSAの「UCSのID」には、UCSAのIDが設定されている。「SAMのID」には、機器のSAMのIDが設定され、UCSAの「SAMのID」には、レシーバ51のSAM62のIDが設定されている。「ユーザのID」には、コンテンツを利用するユーザのIDが設定され、UCSAの「ユーザのID」には、ユーザFのIDが設定されている。

## 【0116】

「利用内容」は、「ID」、「形式」、「パラメータ」、および「管理移動状態情報」の各項目からなり、そのうち「ID」、「形式」、および「パラメータ」の項目には、選択されたUCPの「利用内容」の、それらに対応する項目の情報が設定される。すなわち、UCSAの「ID」には、UCPAの「利用内容13」の「ID13

」に設定されている情報（利用内容 13 の ID）が、「形式」には、「利用内容 13」の「形式 13」に設定されている”期限制限再生”が、「パラメータ」には、「利用内容 13」の「パラメータ 13」に設定されている情報（開始時期および終了時期）が設定されている。

【0117】

「利用内容」の「管理移動状態情報」には、選択された UCP の「管理移動許可情報」に”可”が設定されている場合（管理移動が行える場合）、管理移動元の機器（コンテンツを購入した機器）と管理移動先の機器のそれぞれの ID が設定されるようになされている。なお、コンテンツの管理移動が行われていない状態においては、管理移動元の機器の ID が、管理移動先の機器の ID としても設定される。UCP の「管理移動許可情報」に、”不可”が設定されている場合、「管理移動状態情報」には”不可”が設定される。すなわち、この場合、コンテンツの管理移動は行われず（許可されない）。UCSA の「管理移動状態情報」には、UCPA の「利用内容 13」の「管理移動許可情報 13」に”可”が設定されており、また、このとき、コンテンツ A は管理移動されていないので、SAM 62 の ID が、管理移動元の機器の ID および管理移動先の機器の ID として設定されている。

【0118】

「利用履歴」には、同一のコンテンツに対する利用形式の履歴が含まれている。UCSA の「利用履歴」には、”期限制限再生”を示す情報のみが記憶されているが、例えば、レシーバ 51 において、コンテンツ A が以前に利用されていた場合、そのときの利用形式を示す情報も記憶されている。

【0119】

なお、上述した UCS においては、「UCP の有効期限」および「PT の有効期限」が設けられているがそれらを UCS に設定しないようにすることもできる。また、上述した UCS において、「コンテンツプロバイダの ID」が設けられているが、UCP の ID がユニークで、これにより、コンテンツプロバイダを特定することができる場合、それを設けないようにすることもできる。また「サービスプロバイダの ID」も同様に、PT の ID がユニークで、これにより、サービスプロバイダを特定することができる場合、それを設けないようにすることもできる。

## 【0120】

作成されたUCSは、レシーバ51の復号/暗号化モジュール74の復号化ユニット91から供給されるコンテンツ鍵Kco（保存用鍵Ksaveで暗号化されている）とともに、外部記憶部63に送信され、その利用情報記憶部63Aに記憶される。外部記憶部63の利用情報記憶部63Aは、図22に示すように、M個のブロックBP-1乃至BP-Mに分割され（例えば、1メガバイト毎に分割され）、各ブロックBPが、N個の利用情報用メモリ領域RP-1乃至RP-Nに分割されている。SAM62から供給されるコンテンツ鍵Kco（保存用鍵Ksaveで暗号化されている）およびUCSは、利用情報用記憶部63Aの所定のブロックBPの利用情報用メモリ領域RPに、対応して記憶される。

## 【0121】

図22の例では、ブロックBP-1の利用情報用メモリ領域RP-3に、図21に示したUCSAと、コンテンツ鍵KcoA（保存用鍵Ksaveで暗号化されている）が対応して記憶されている。ブロックBP-1の利用情報用メモリ領域RP-1、RP-2には、他のコンテンツ鍵Kco1、Kco2（それぞれ保存用鍵Ksaveで暗号化されている）およびUCS1、2がそれぞれ記憶されている。ブロックBP-1の利用情報用メモリ領域RP-4（図示せず）乃至RP-N、およびブロックBP-2（図示せず）乃至BP-Mには、この場合、コンテンツ鍵KcoおよびUCSは記憶されておらず、空いていることを示す所定の初期情報が記憶されている。なお、利用情報用メモリ領域RPに記憶されるコンテンツ鍵Kco（保存用鍵Ksaveで暗号化されている）およびUCSを、個々に区別する必要がない場合、まとめて、利用情報と称する。

## 【0122】

図23は、図21に示したUCSAと同時に作成された課金情報Aを表している。課金情報には、図23に示されるように、「コンテンツのID」、「コンテンツプロバイダのID」、「UCPのID」、「UCPの有効期限」、「サービスプロバイダのID」、「PTのID」、「PTの有効期限」、「UCSのID」、「SAMのID」、「ユーザのID」、および「利用内容」の各項目に設定される所定の情報が含まれる。

## 【0123】

課金情報の、「コンテンツのID」、「コンテンツプロバイダのID」、「UCPのID」、「UCPの有効期限」、「サービスプロバイダのID」、「PTのID」、「PTの有効期限」、「UCSのID」、「SAMのID」、「ユーザのID」、および「利用内容」には、UCSの、それらに対応する項目の情報が、それぞれ設定される。すなわち、図23の課金情報Aの、「コンテンツのID」には、コンテンツAのIDが、「コンテンツプロバイダのID」には、コンテンツプロバイダ2のIDが、「UCPのID」には、UCPAのIDが、「UCPの有効期限」には、UCPAの有効期限が、「サービスプロバイダのID」には、サービスプロバイダ3のIDが、「PTのID」には、PTA-1のIDが、「PTの有効期限」には、PTA-1の有効期限が、「UCSのID」には、UCSAのIDが、「SAMのID」には、SAM62のIDが、「ユーザのID」には、レシーバ51のユーザFのIDが、そして「利用内容」には、UCSAの「利用内容13」の内容が、それぞれ設定されている。

## 【0124】

なお、上述した課金情報においては、「UCPの有効期限」および「PTの有効期限」が、設けられているがそれらをUCSに設定しないようにすることもできる。また、上述した課金情報において、「コンテンツプロバイダのID」が設けられているが、UCPのIDがユニークで、これにより、コンテンツプロバイダを特定することができる場合、それを設けないようにすることもできる。また「サービスプロバイダのID」も同様に、PTのIDがユニークで、これにより、サービスプロバイダを特定することができる場合、それを設けないようにすることもできる。

## 【0125】

図19に戻り、記憶モジュール73には、図24に示すように、SAM62の公開鍵K<sub>pu</sub>、SAM62の秘密鍵K<sub>su</sub>、EMDサービスセンタ1の公開鍵K<sub>pesc</sub>、認証局の公開鍵K<sub>pca</sub>、保存用鍵K<sub>save</sub>、3月分の配送用鍵K<sub>d</sub>などの各種鍵、SAM62の証明書、課金情報（例えば、図23の課金情報A）、基準情報51、およびM個の検査値HP-1乃至HP-Mなどが記憶されている。

## 【0126】

記憶モジュール73に記憶される検査値HP-1は、外部記憶部63の利用情報記憶部63A（図22）のブロックBP-1に記憶されているデータの全体に



ハッシュ関数が適用されて算出されたハッシュ値である。検査値HP-2乃至HP-Mも、検査値HP-1と同様に、外部記憶部63の、対応するブロックBP-2乃至BP-Mのそれぞれに記憶されているデータにハッシュ関数が適用されて算出されたハッシュ値である。

#### 【0127】

図25は、記憶モジュール73に記憶されている基準情報51を表している。基準情報には、「SAMのID」、「機器番号」、「決済ID」、「課金の上限額」、「決済ユーザ情報」、「従属ユーザ情報」、および「利用ポイント情報」の各項目に設定される所定の情報が含まれる。

#### 【0128】

基準情報の、「SAMのID」、「機器番号」、「決済ID」、「決済ユーザ情報」、「従属ユーザ情報」、および「利用ポイント情報」には、EMDサービスセンタ1のユーザ管理部18により管理されているシステム登録情報の、SAM62のIDに対応する項目の情報が設定される。すなわち、基準情報51には、SAM62のID、SAM62の機器番号(100番)、ユーザFの決済ID、ユーザFの決済ユーザ情報(ユーザFの一般情報(氏名、住所、電話番号、決済機関情報、生年月日、年齢、性別)、ユーザFのID、およびユーザFのパスワード)、およびレシーバ51の利用ポイント情報が設定されている。

#### 【0129】

「課金の上限額」には、機器がEMDシステム正式登録されている状態と仮登録されている状態で、それぞれ異なる額を示す、課金の上限額が設定されている。基準情報51の「課金の上限額」には、レシーバ51が正式登録されているので、正式登録されている状態における課金の上限額を示す情報(“正式登録時の上限額”)が設定されている。

#### 【0130】

図19に戻り、SAM62の復号/暗号化モジュール74は、復号ユニット91、乱数発生ユニット92、および暗号化ユニット93から構成される。復号ユニット91は、暗号化されたコンテンツ鍵Kcを配送用鍵Kdで復号し、暗号化ユニット93に出力する。乱数発生ユニット92は、相互認証時に、所定の桁数

の乱数を発生し、必要に応じて一時鍵  $K_{temp}$  を生成し、暗号化ユニット 93 に出力する。

#### 【0131】

暗号化ユニット 93 は、復号されたコンテンツ鍵  $K_c$  を、再度、記憶モジュール 73 に保持されている保存用鍵  $K_{save}$  で暗号化する。暗号化されたコンテンツ鍵  $K_c$  は、外部記憶部 63 に供給される。暗号化ユニット 93 は、コンテンツ鍵  $K_c$  を伸張部 64 に送信するとき、コンテンツ鍵  $K_c$  を乱数発生ユニット 92 で生成した一時鍵  $K_{temp}$  で暗号化する。

#### 【0132】

データ検査モジュール 75 は、記憶モジュール 73 に記憶されている検査値  $H_P$  と、外部記憶部 63 の利用情報記憶部 63A の、対応するブロック BP のデータのハッシュ値を比較し、ブロック BP のデータが改竄されていないか否かを検査する。

#### 【0133】

伸張部 64 は、相互認証モジュール 101、復号モジュール 102、復号モジュール 103、伸張モジュール 104、およびウォーターマーク付加モジュール 105 から構成される。相互認証モジュール 101 は、SAM 62 と相互認証し、一時鍵  $K_{temp}$  を復号モジュール 102 に出力する。復号モジュール 102 は、一時鍵  $K_{temp}$  で暗号化されたコンテンツ鍵  $K_c$  を一時鍵  $K_{temp}$  で復号し、復号モジュール 103 に出力する。復号モジュール 103 は、HDD 52 に記録されたコンテンツをコンテンツ鍵  $K_c$  で復号し、伸張モジュール 104 に出力する。伸張モジュール 104 は、復号されたコンテンツを、更に ATRAC2 等の方式で伸張し、ウォーターマーク付加モジュール 105 に出力する。ウォーターマーク付加モジュール 105 は、コンテンツにレシーバ 51 を特定する所定のウォーターマーク（電子透かし）を挿入し、図示せぬスピーカに出力し、音楽を再生する。

#### 【0134】

通信部 65 は、ユーザホームネットワーク 5 のレシーバ 201 およびレシーバ 301 との通信処理を行う。インターフェース 66 は、SAM 62 および伸張部 64 からの信号を所定の形式に変更し、HDD 52 に出力し、また、HDD 52 からの信

号を所定の形式に変更し、SAM 6 2 および伸張部 6 4 に出力する。

【0135】

表示制御部 6 7 は、表示部（図示せず）への出力を制御する。入力制御部 6 8 は、各種ボタンなどから構成される操作部（図示せず）からの入力を制御する。

【0136】

HDD 5 2 は、サービスプロバイダ 3 から供給されたコンテンツなどを記憶する他、図 2 6 に示すような登録リストを記憶している。この登録リストは、表形式に情報が記憶されているリスト部、および登録リストを保持する機器についての所定の情報が記憶されている対象SAM情報部より構成されている。

【0137】

対象SAM情報部には、この登録リストを保有する機器のSAMID、この例の場合、レシーバ 5 1 のSAM 6 2 のIDが（「対象SAMID」の欄に）記憶されている。対象SAM情報部にはまた、この登録リストの有効期限が（「有効期限」の欄に）記憶され、登録リストのバージョン番号が（「バージョン番号」の欄に）記憶され、そして接続されている機器の数（自分自身を含む）、この例の場合、レシーバ 5 1 には、レシーバ 2 0 1 およびレシーバ 3 0 1 の 2 機の機器が接続されているので、自分自身を含む合計値 3 が（「接続されている機器数」の欄に）記憶されている。

【0138】

リスト部は、「SAMID」、「ユーザID」、「購入処理」、「課金処理」、「課金機器」、「コンテンツ供給機器」、「状態フラグ」、「登録条件署名」、および「登録リスト署名」の 9 個の項目から構成され、この例の場合、レシーバ 5 1 の登録条件、レシーバ 2 0 1 の登録条件、およびレシーバ 3 0 1 の登録条件が記憶されている。

【0139】

「SAMID」には、機器のSAMのIDが記憶される。この例の場合、レシーバ 5 1 のSAM 6 2 のID、レシーバ 2 0 1 のSAM 2 1 2 のID、およびレシーバ 3 0 1 のSAM 3 1 1 のIDが記憶されている。「ユーザID」には、決済ユーザのIDが記憶される。この例の場合、ユーザ F のIDが、レシーバ 5 1、レシーバ 2 0 1、およびレシー

バ 3 0 1 に対応する「ユーザID」に、それぞれ記憶されている。

【0140】

「購入処理」には、機器が、コンテンツを購入するための処理を行うことができるか否かを示す情報（”可”または”不可”）が記憶される。この例の場合、レシーバ 5 1 およびレシーバ 2 0 1 は、コンテンツを購入するための処理を行うことができるようになされているので、それらに対応する「購入処理」には、”可”が記憶されている。レシーバ 3 0 1 は、購入処理を行うことができないものとされているので、対応する「購入処理」には、”不可”が記憶されている。

【0141】

「課金処理」には、機器が、EMDサービスセンタ 1 との間で、課金処理を行うことができるか否かを示す情報（”可”または”不可”）が記憶される。この例の場合、レシーバ 5 1 およびレシーバ 2 0 1 は、課金処理を行うことができようになされているので、それらに対応する「課金処理」には、それぞれ”可”が記憶される。レシーバ 3 0 1 は、課金処理を行うことができないものとされているので、対応する「課金処理」には、”不可”が記憶されている。

【0142】

「課金機器」には、計上された課金を決済する処理を行う機器のSAMのIDが記憶される。この例の場合、レシーバ 5 1 およびレシーバ 2 0 1 は、自分自身で課金処理を行うことができるので、それらに対応する「課金機器」には、自分自身のSAMのIDが記憶されている。レシーバ 3 0 1 は、コンテンツの購入および課金も行われないので、対応する「課金機器」には、”なし”が記憶されている。

【0143】

「コンテンツ供給機器」には、機器が、コンテンツの供給をサービスプロバイダ 3 からではなく、接続される他の機器から受ける場合、コンテンツを供給することができる機器のSAMのIDが記憶される。この例の場合、レシーバ 5 1 は、コンテンツの供給をサービスプロバイダ 3 から受けるので、「コンテンツ供給機器」には、コンテンツを供給する機器が存在しないことを示す情報（”なし”）が記憶されている。レシーバ 2 0 1 およびレシーバ 3 0 1 は、コンテンツの供給をレシーバ 5 1 から受けるので、対応する「コンテンツ供給機器」には、レシーバ

51のSAM62のIDが設定されている。

【0144】

「状態フラグ」には、機器の動作制限条件が記憶される。何ら制限されていない場合は、その旨を示す情報（”制限なし”）、一定の制限が課せられている場合は、その旨を示す情報（”制限あり”）、また動作が停止される場合には、その旨を示す情報（”停止”）が記憶される。例えば、課金の決済が成功しなかった場合、その機器に対応する「状態フラグ」には、”制限あり”が設定される。この例の場合、「状態フラグ」に”制限あり”が設定された機器においては、すでに購入されたコンテンツを利用するための処理は実行されるが、新たなコンテンツを購入するための処理は実行されなくなる。すなわち、一定の制限が機器に課せられる。また、コンテンツの不正複製などの違反行為が発覚した場合、「状態フラグ」には、”停止”が設定され、機器の動作が停止される。これにより、その機器はEMDシステムからのサービスを、一切受けることができなくなる。

【0145】

この例の場合、レシーバ51、レシーバ201、およびレシーバ301に対しては、何ら制限が課せられていないものとし、それぞれに対応する「状態フラグ」には、”なし”が設定されている。なお、「状態フラグ」に設定される、”制限あり”および”停止”など、これにより動作が制限される情報を、個々に区別する必要がない場合、まとめて、動作制限情報と称する。

【0146】

「登録条件署名」には、上述したように、各登録条件として、それぞれ、「SAMID」、「ユーザID」、「購入処理」、「課金処理」、「課金機器」、「コンテンツ供給機器」、および「状態フラグ」に記憶されている情報に対するEMDサービスセンタ1による署名が記憶されている。「登録リスト署名」には、登録リストに設定されているデータの全体に対する署名が記憶されている。

【0147】

図27は、レシーバ201の構成例を表している。レシーバ201の通信部211乃至入力制御部218は、レシーバ51の通信部61乃至入力制御部68と同様の機能を有しているので、その詳細な説明は適宜省略するが、レシーバ20

1の記憶モジュール223には、図28に示すような基準情報201が記憶されている。基準情報201には、EMDサービスセンタ1のユーザ管理部18により管理されているシステム登録情報の、SAM212のIDに対応して記憶されている、SAM212のID、レシーバ201の機器番号（100番）、ユーザFの決済ID、ユーザFの決済ユーザ情報（ユーザFの一般情報（氏名、住所、電話番号、決済機関情報、生年月日、年齢、性別）、ユーザFのID、およびユーザFのパスワード）、ユーザAの従属ユーザ情報（ユーザAの一般情報（氏名、住所、電話番号、生年月日、性別）、ユーザAのID、およびユーザAのパスワード）、およびレシーバ201の利用ポイント情報が設定されている。「課金の上限額」には、「正式登録時の上限額」が設定されている。

#### 【0148】

HDD202も、HDD51に記憶されている情報が記憶されているので、その説明は省略するが、図29に示すようなレシーバ201の登録リストが記憶されている。この登録リストの対象SAM情報部には、レシーバ201のSAM212のID、その登録リストの有効期限、バージョン番号、接続されている機器の数（この例では、レシーバ201には、レシーバ51の1機が接続されているので、自分自身を含めた合計数2）が記憶されている。リスト部には、図26のレシーバ51の登録リストの、レシーバ51およびレシーバ201の登録条件が記憶されている。

#### 【0149】

図30は、レシーバ301の機能的構成例を表している。レシーバ301は、レシーバ201のSAM212乃至通信部215と基本的に同様の機能を有する、SAM311乃至通信部314を有しているが、レシーバ201の、通信部211、インタフェース216、表示制御部217、および入力制御部218に対応する機能を有しない、携帯型の機器である。

#### 【0150】

図31は、レシーバ301の記憶モジュール323に記憶されている基準情報301を表している。基準情報301には、EMDサービスセンタ1のユーザ管理部18により管理されているシステム登録情報の、SAM311のIDに対応して記

憶されている、SAM311のID、SAM311の機器番号（25番）、ユーザFの決済ID、ユーザFの決済ユーザ情報（ユーザFの一般情報（氏名、住所、電話番号、決済機関情報、生年月日、年齢、性別）、ユーザFのID、およびユーザFのパスワード）、ユーザAの従属ユーザ情報（ユーザAの一般情報（氏名、住所、電話番号、生年月日、性別）、ユーザAのID、およびユーザAのパスワード）、およびレシーバ301の利用ポイント情報が設定されている。「課金の上限額」には、レシーバ301が正式登録されているので、正式登録されている状態における課金の上限額を示す情報（「正式登録時の上限額」）が設定されている。

#### 【0151】

図32に示すようなレシーバ301の登録リストは、記憶モジュール323に記憶されている。この登録リストの対象SAM情報部には、この登録リストを保有するレシーバ301のSAM311のIDが（「対象SAMID」の欄に）記憶され、その登録リストの有効期限が（「有効期限」の欄に）記憶され、登録リストのバージョン番号が（「バージョン番号」の欄に）記憶され、そして接続されている機器の数（自分自身を含む）、この例の場合、レシーバ301には、レシーバ51の1機の機器が接続されているので、自分自身を含む合計数2が（「接続されている機器数」の欄に）記憶されている。リスト部には、図26のレシーバ51の登録リストの、レシーバ301の登録条件が記憶されているが、この場合、「登録条件署名」および「登録リスト署名」は、削除されている。これは、登録リストの署名の確認後、取り除かれたためで、これにより、記憶モジュール323の記憶容量を節約することができる。なお、この例の場合、1つの署名あたり、40バイトが必要とされる。

#### 【0152】

次に、EMDシステムの処理について、図33のフローチャートを参照して説明するが、なお、ここでは、ユーザFが、レシーバ51を介して、コンテンツAを購入し、利用する場合を例として説明する。

#### 【0153】

ステップS11において、配送用鍵Kdが、EMDサービスセンタ1からコンテンツプロバイダ2に供給されるが、この処理の詳細は、図34のフローチャート

に示されている。すなわち、ステップ S 3 1 において、EMD サービスセンタ 1 の相互認証部 1 7 は、コンテンツプロバイダ 2 の相互認証部 3 9 と相互認証し、コンテンツプロバイダ 2 が、正当なプロバイダであることが確認された後、EMD サービスセンタ 1 のコンテンツプロバイダ管理部 1 2 は、鍵サーバ 1 4 から供給された配送用鍵 K d をコンテンツプロバイダ 2 に送信する。なお、相互認証処理の詳細は、図 3 5 乃至図 3 7 を参照して後述する。

#### 【0154】

次に、ステップ S 3 2 において、コンテンツプロバイダ 2 の暗号化部 3 6 は、EMD サービスセンタ 1 から送信された配送用鍵 K d を受信し、ステップ S 3 3 において、記憶する。

#### 【0155】

このように、コンテンツプロバイダ 2 の暗号化部 3 6 が、配送用鍵 K d を記憶したとき、処理は終了し、図 3 3 のステップ S 1 2 に進む。ここで、ステップ S 1 2 の処理の説明の前に、図 3 4 のステップ S 3 1 における相互認証処理（なりすましがいないことを確認する処理）について、1 つの共通鍵を用いる場合（図 3 5）、2 つの共通鍵を用いる場合（図 3 6）、および公開鍵暗号を用いる場合（図 3 7）を例として説明する。

#### 【0156】

図 3 5 は、1 つの共通鍵で、共通鍵暗号である DES を用いる、コンテンツプロバイダ 2 の相互認証部 3 9 と EMD サービスセンタ 1 の相互認証部 1 7 との相互認証の動作を説明するフローチャートである。ステップ S 4 1 において、コンテンツプロバイダ 2 の相互認証部 3 9 は、64 ビットの乱数 R 1 を生成する（乱数生成部 3 5 が生成するようにしてもよい）。ステップ S 4 2 において、コンテンツプロバイダ 2 の相互認証部 3 9 は、DES を用いて乱数 R 1 を、予め記憶している共通鍵 K c で暗号化する（暗号化部 3 6 で暗号化するようにしてもよい）。ステップ S 4 3 において、コンテンツプロバイダ 2 の相互認証部 3 9 は、暗号化された乱数 R 1 を EMD サービスセンタ 1 の相互認証部 1 7 に送信する。

#### 【0157】

ステップ S 4 4 において、EMD サービスセンタ 1 の相互認証部 1 7 は、受信し



た乱数  $R_1$  を予め記憶している共通鍵  $K_c$  で復号する。ステップ S45 において、EMD サービスセンタ 1 の相互認証部 17 は、32 ビットの乱数  $R_2$  を生成する。ステップ S46 において、EMD サービスセンタ 1 の相互認証部 17 は、復号した 64 ビットの乱数  $R_1$  の下位 32 ビットを乱数  $R_2$  で入れ替え、接続  $R_{1H} \parallel R_2$  を生成する。なお、ここで  $R_{iH}$  は、 $R_i$  の上位ビットを表し、 $A \parallel B$  は、 $A$  と  $B$  の接続 ( $n$  ビットの  $A$  の下位に、 $m$  ビットの  $B$  を結合して、 $(n+m)$  ビットとしたもの) を表す。ステップ S47 において、EMD サービスセンタ 1 の相互認証部 17 は、DES を用いて  $R_{1H} \parallel R_2$  を共通鍵  $K_c$  で暗号化する。ステップ S48 において、EMD サービスセンタ 1 の相互認証部 17 は、暗号化した  $R_{1H} \parallel R_2$  をコンテンツプロバイダ 2 に送信する。

## 【0158】

ステップ S49 において、コンテンツプロバイダ 2 の相互認証部 39 は、受信した  $R_{1H} \parallel R_2$  を共通鍵  $K_c$  で復号する。ステップ S50 において、コンテンツプロバイダ 2 の相互認証部 39 は、復号した  $R_{1H} \parallel R_2$  の上位 32 ビット  $R_{1H}$  を調べ、ステップ S41 で生成した、乱数  $R_1$  の上位 32 ビット  $R_{1H}$  と一致すれば、EMD サービスセンタ 1 が正当なセンタであることを認証する。生成した乱数  $R_{1H}$  と、受信した  $R_{1H}$  が一致しないとき、処理は終了される。両者が一致するとき、ステップ S51 において、コンテンツプロバイダ 2 の相互認証部 39 は、32 ビットの乱数  $R_3$  を生成する。ステップ S52 において、コンテンツプロバイダ 2 の相互認証部 39 は、受信し、復号した 32 ビットの乱数  $R_2$  を上位に設定し、生成した乱数  $R_3$  をその下位に設定し、接続  $R_2 \parallel R_3$  とする。ステップ S53 において、コンテンツプロバイダ 2 の相互認証部 39 は、DES を用いて接続  $R_2 \parallel R_3$  を共通鍵  $K_c$  で暗号化する。ステップ S54 において、コンテンツプロバイダ 2 の相互認証部 39 は、暗号化された接続  $R_2 \parallel R_3$  を EMD サービスセンタ 1 の相互認証部 17 に送信する。

## 【0159】

ステップ S55 において、EMD サービスセンタ 1 の相互認証部 17 は、受信した接続  $R_2 \parallel R_3$  を共通鍵  $K_c$  で復号する。ステップ S56 において、EMD サービスセンタ 1 の相互認証部 17 は、復号した接続  $R_2 \parallel R_3$  の上位 32 ビットを調

べ、乱数 R 2 と一致すれば、コンテンツプロバイダ 2 を正当なプロバイダとして認証し、一致しなければ、不正なプロバイダとして、処理を終了する。

## 【0160】

図 36 は、2 つの共通鍵 K c 1, K c 2 で、共通鍵暗号である DES を用いる、コンテンツプロバイダ 2 の相互認証部 39 と EMD サービスセンタ 1 の相互認証部 17 との相互認証の動作を説明するフローチャートである。ステップ S 61 において、コンテンツプロバイダ 2 の相互認証部 39 は、64 ビットの乱数 R 1 を生成する。ステップ S 62 において、コンテンツプロバイダ 2 の相互認証部 39 は、DES を用いて乱数 R 1 を予め記憶している共通鍵 K c 1 で暗号化する。ステップ S 63 において、コンテンツプロバイダ 2 の相互認証部 39 は、暗号化された乱数 R 1 を EMD サービスセンタ 1 に送信する。

## 【0161】

ステップ S 64 において、EMD サービスセンタ 1 の相互認証部 17 は、受信した乱数 R 1 を予め記憶している共通鍵 K c 1 で復号する。ステップ S 65 において、EMD サービスセンタ 1 の相互認証部 17 は、乱数 R 1 を予め記憶している共通鍵 K c 2 で暗号化する。ステップ S 66 において、EMD サービスセンタ 1 の相互認証部 17 は、64 ビットの乱数 R 2 を生成する。ステップ S 67 において、EMD サービスセンタ 1 の相互認証部 17 は、乱数 R 2 を共通鍵 K c 2 で暗号化する。ステップ S 68 において、EMD サービスセンタ 1 の相互認証部 17 は、暗号化された乱数 R 1 および乱数 R 2 をコンテンツプロバイダ 2 の相互認証部 39 に送信する。

## 【0162】

ステップ S 69 において、コンテンツプロバイダ 2 の相互認証部 39 は、受信した乱数 R 1 および乱数 R 2 を予め記憶している共通鍵 K c 2 で復号する。ステップ S 70 において、コンテンツプロバイダ 2 の相互認証部 39 は、復号した乱数 R 1 を調べ、ステップ S 61 で生成した乱数 R 1 (暗号化する前の乱数 R 1) と一致すれば、EMD サービスセンタ 1 を適正なセンタとして認証し、一致しなければ、不正なセンタであるとして、処理を終了する。ステップ S 71 において、コンテンツプロバイダ 2 の相互認証部 39 は、復号して得た乱数 R 2 を共通鍵 K

c 1で暗号化する。ステップS 72において、コンテンツプロバイダ2の相互認証部39は、暗号化された乱数R 2をEMDサービスセンタ1に送信する。

【0163】

ステップS 73において、EMDサービスセンタ1の相互認証部17は、受信した乱数R 2を共通鍵K c 1で復号する。ステップS 74において、EMDサービスセンタ1の相互認証部17は、復号した乱数R 2が、ステップS 66で生成した乱数R 2（暗号化する前の乱数R 2）と一致すれば、コンテンツプロバイダ2を適正なプロバイダとして認証し、一致しなければ、不正なプロバイダであるとして処理を終了する。

【0164】

図37は、公開鍵暗号である、160ビット長の楕円曲線暗号を用いる、コンテンツプロバイダ2の相互認証部39とEMDサービスセンタ1の相互認証部17との相互認証の動作を説明するフローチャートである。ステップS 81において、コンテンツプロバイダ2の相互認証部39は、64ビットの乱数R 1を生成する。ステップS 82において、コンテンツプロバイダ2の相互認証部39は、自分自身の公開鍵K p c pを含む証明書（認証局から予め取得しておいたもの）と、乱数R 1をEMDサービスセンタ1の相互認証部17に送信する。

【0165】

ステップS 83において、EMDサービスセンタ1の相互認証部17は、受信した証明書の署名（認証局の秘密鍵K s c aで暗号化されている）を、予め取得しておいた認証局の公開鍵K p c aで復号し、コンテンツプロバイダ2の公開鍵K p c pとコンテンツプロバイダ2の名前のハッシュ値を取り出すとともに、証明書に平文のまま格納されているコンテンツプロバイダ2の公開鍵K p c pおよびコンテンツプロバイダ2の名前を取り出す。証明書が認証局が発行した適正なものであるならば、証明書の署名を復号することが可能であり、復号して得られた公開鍵K p c pおよびコンテンツプロバイダ2の名前のハッシュ値は、平文のまま証明書に格納されていたコンテンツプロバイダ2の公開鍵K p c pおよびコンテンツプロバイダ2の名前にハッシュ関数を適用して得られたハッシュ値と一致する。これにより、公開鍵K p c pが改竄されたものでない適正なものであることが

認証される。署名を復号出来なかったり、できたとしてもハッシュ値が一致しないときには、適正な公開鍵でないか、適正なプロバイダでないことになる。この時処理は終了される。

#### 【0166】

適正な認証結果が得られたとき、ステップS84において、EMDサービスセンタ1の相互認証部17は、64ビットの乱数R2を生成する。ステップS85において、EMDサービスセンタ1の相互認証部17は、乱数R1および乱数R2の接続 $R1 \parallel R2$ を生成する。ステップS86において、EMDサービスセンタ1の相互認証部17は、接続 $R1 \parallel R2$ を自分自身の秘密鍵 $K_{sec}$ で暗号化する。ステップS87において、EMDサービスセンタ1の相互認証部17は、接続 $R1 \parallel R2$ を、ステップS83で取得したコンテンツプロバイダ2の公開鍵 $K_{cp}$ で暗号化する。ステップS88において、EMDサービスセンタ1の相互認証部17は、秘密鍵 $K_{sec}$ で暗号化された接続 $R1 \parallel R2$ 、公開鍵 $K_{cp}$ で暗号化された接続 $R1 \parallel R2$ 、および自分自身の公開鍵 $K_{pe}$ を含む証明書（認証局から予め取得しておいたもの）をコンテンツプロバイダ2の相互認証部39に送信する。

#### 【0167】

ステップS89において、コンテンツプロバイダ2の相互認証部39は、受信した証明書の署名を予め取得しておいた認証局の公開鍵 $K_{pa}$ で復号し、正しければ証明書から公開鍵 $K_{pe}$ を取り出す。この場合の処理は、ステップS83における場合と同様であるので、その説明は省略する。ステップS90において、コンテンツプロバイダ2の相互認証部39は、EMDサービスセンタ1の秘密鍵 $K_{sec}$ で暗号化されている接続 $R1 \parallel R2$ を、ステップS89で取得した公開鍵 $K_{pe}$ で復号する。ステップS91において、コンテンツプロバイダ2の相互認証部39は、自分自身の公開鍵 $K_{cp}$ で暗号化されている接続 $R1 \parallel R2$ を、自分自身の秘密鍵 $K_{sc}$ で復号する。ステップS92において、コンテンツプロバイダ2の相互認証部39は、ステップS90で復号された接続 $R1 \parallel R2$ と、ステップS91で復号された接続 $R1 \parallel R2$ を比較し、一致すればEMDサービスセンタ1を適正なものとして認証し、一致しなければ、不適正な

ものとして、処理を終了する。

【0 1 6 8】

適正な認証結果が得られたとき、ステップ S 9 3 において、コンテンツプロバイダ 2 の相互認証部 3 9 は、6 4 ビットの乱数 R 3 を生成する。ステップ S 9 4 において、コンテンツプロバイダ 2 の相互認証部 3 9 は、ステップ S 9 0 で取得した乱数 R 2 および生成した乱数 R 3 の接続  $R 2 \parallel R 3$  を生成する。ステップ S 9 5 において、コンテンツプロバイダ 2 の相互認証部 3 9 は、接続  $R 2 \parallel R 3$  を、ステップ S 8 9 で取得した公開鍵  $K_{p e s c}$  で暗号化する。ステップ S 9 6 において、コンテンツプロバイダ 2 の相互認証部 3 9 は、暗号化した接続  $R 2 \parallel R 3$  を EMD サービスセンタ 1 の相互認証部 1 7 に送信する。

【0 1 6 9】

ステップ S 9 7 において、EMD サービスセンタ 1 の相互認証部 1 7 は、暗号化された接続  $R 2 \parallel R 3$  を自分自身の秘密鍵  $K_{s e s c}$  で復号する。ステップ S 9 8 において、EMD サービスセンタ 1 の相互認証部 1 7 は、復号した乱数 R 2 が、ステップ S 8 4 で生成した乱数 R 2（暗号化する前の乱数 R 2）と一致すれば、コンテンツプロバイダ 2 を適正なプロバイダとして認証し、一致しなければ、不適正なプロバイダとして、処理を終了する。

【0 1 7 0】

以上のように、EMD サービスセンタ 1 の相互認証部 1 7 とコンテンツプロバイダ 2 の相互認証部 3 9 は、相互認証する。相互認証に利用された乱数は、その相互認証に続く処理にだけ有効な一時鍵  $K_{t e m p}$  として利用される。

【0 1 7 1】

次に、図 3 3 のステップ S 1 2 の処理について説明する。ステップ S 1 2 においては、コンテンツプロバイダセキュアコンテナが、コンテンツプロバイダ 2 からサービスプロバイダ 3 に供給される。その処理の詳細は、図 3 8 のフローチャートに示されている。すなわち、ステップ S 2 0 1 において、コンテンツプロバイダ 2 のウォーターマーク付加部 3 2（図 9）は、コンテンツサーバ 3 1 からコンテンツ A を読み出し、コンテンツプロバイダ 2 を示す所定のウォーターマーク（電子透かし）を挿入し、圧縮部 3 3 に供給する。

## 【0172】

ステップS202において、コンテンツプロバイダ2の圧縮部33は、ウォーターマークが挿入されたコンテンツAをATRAC2等の所定の方式で圧縮し、暗号化部34に供給する。ステップS203において、乱数発生部35は、コンテンツ鍵Kc o Aとなる乱数を発生させ、暗号化部34に供給する。

## 【0173】

ステップS204において、コンテンツプロバイダ2の暗号化部34は、DESなどの所定の方式で、乱数発生部35で発生された乱数（コンテンツ鍵Kc o A）を使用して、ウォーターマークが挿入されて圧縮されたコンテンツAを暗号化する。次に、ステップS205において、暗号化部36は、DESなどの所定の方式で、EMDサービスセンタ1から供給された配送用鍵Kdでコンテンツ鍵Kc o Aを暗号化する。

## 【0174】

ステップS206において、コンテンツプロバイダ2のセキュアコンテナ作成部38は、コンテンツA（コンテンツ鍵Kc o Aで暗号化されている）、コンテンツ鍵Kc o A（配送用鍵Kdで暗号化されている）、およびコンテンツAに対応するUCPAの全体にハッシュ関数を適用してハッシュ値を算出し、自分自身の秘密鍵Ks c pで暗号化する。これにより、図13に示した署名が作成される。

## 【0175】

ステップS207において、コンテンツプロバイダ2のセキュアコンテナ作成部38は、コンテンツA（コンテンツ鍵Kc o Aで暗号化されている）、コンテンツ鍵Kc o A（配送用鍵Kdで暗号化されている）、UCPA、およびステップS206で生成した署名を含んだ、図13に示したコンテンツプロバイダセキュアコンテナを作成する。

## 【0176】

ステップS208において、コンテンツプロバイダ2の相互認証部39は、サービスプロバイダ3の相互認証部45と相互認証する。この認証処理は、図35乃至図37を参照して説明した場合と同様であるので、その説明は省略する。ステップS209において、コンテンツプロバイダ2のセキュアコンテナ作成部3

8は、認証局から予め発行された証明書を、ステップS207で作成したコンテンツプロバイダセキュアコンテナに付して、サービスプロバイダ3に送信する。

【0177】

このようにして、コンテンツプロバイダセキュアコンテナが、サービスプロバイダ3に供給されたとき、処理は終了し、図33のステップS13に進む。

【0178】

ステップS13において、サービスプロバイダセキュアコンテナが、サービスプロバイダ3からユーザホームネットワーク5（レシーバ51）に供給される。この処理の詳細は、図39のフローチャートに示されている。すなわち、ステップS221において、サービスプロバイダ3の値付け部42は、コンテンツプロバイダ2から送信されたコンテンツプロバイダセキュアコンテナに付された証明書に含まれる署名を確認し、証明書の改竄がなければ、それから、コンテンツプロバイダ2の公開鍵 $K_{p,c,p}$ を取り出す。証明書の署名の確認は、図37のステップS83における処理と同様であるので、その説明は省略する。

【0179】

ステップS222において、サービスプロバイダ3の値付け部42は、コンテンツプロバイダ2から送信されたコンテンツプロバイダセキュアコンテナの署名をコンテンツプロバイダ2の公開鍵 $K_{p,c,p}$ で復号し、得られたハッシュ値が、コンテンツA（コンテンツ鍵 $K_{c,o,A}$ で暗号化されている）、コンテンツ鍵 $K_{c,o,A}$ （配送用鍵 $K_d$ で暗号化されている）、およびUCPAの全体にハッシュ関数を適用して得られたハッシュ値と一致するか否かを判定し、コンテンツプロバイダセキュアコンテナの改竄がないことを確認する。両者の値が一致しない場合（改竄が発見された場合）は、処理は終了されるが、この例の場合、コンテンツプロバイダセキュアコンテナの改竄はなかったものとし、ステップS223に進む。

【0180】

ステップS223において、サービスプロバイダ3の値付け部42は、コンテンツプロバイダセキュアコンテナから、コンテンツA（コンテンツ鍵 $K_{c,o,A}$ で暗号化されている）、コンテンツ鍵 $K_{c,o,A}$ （配送用鍵 $K_d$ で暗号化されている）

）、およびコンテンツプロバイダ2の署名を取り出し、コンテンツサーバ41に供給する。コンテンツサーバ41は、それらを記憶する。値付け部42はまたUCPAも、コンテンツプロバイダセキュアコンテナから取り出し、セキュアコンテナ作成部44に供給する。

【0181】

ステップS224において、サービスプロバイダ3の値付け部42は、取り出したUCPAに基づいて、PTA-1、A-2を作成し、セキュアコンテナ作成部44に供給する。

【0182】

ステップS225において、サービスプロバイダ3のセキュアコンテナ作成部44は、コンテンツA（コンテンツ鍵Kc o Aで暗号化されている）、コンテンツ鍵Kc o A（配送用鍵Kdで暗号化されている）、コンテンツプロバイダ2の署名、UCPA、PTA-1、A-2、およびサービスプロバイダ3の署名から、図17に示したサービスプロバイダセキュアコンテナを作成する。

【0183】

ステップS226において、サービスプロバイダ3の相互認証部45は、レシーバ51の相互認証モジュール71と相互認証する。この認証処理は、図35乃至図37を参照して説明した場合と同様であるので、その説明を省略する。

【0184】

ステップS227において、サービスプロバイダ3のセキュアコンテナ作成部44は、ステップS225で作成したサービスプロバイダセキュアコンテナに、サービスプロバイダ3の証明書を付して、ユーザホームネットワーク5のレシーバ51に送信する。

【0185】

このようにして、サービスプロバイダセキュアコンテナが、サービスプロバイダ3からレシーバ51に送信されたとき、処理は終了し、図33のステップS14に進む。

【0186】

ステップS14において、サービスプロバイダ3から送信されたサービスプロ



バイダセキュアコンテナが、ユーザホームネットワーク 5 のレシーバ 5 1 により受信される。この処理の詳細は、図 40 のフローチャートに示されている。すなわち、ステップ S 2 4 1 において、レシーバ 5 1 の相互認証モジュール 7 1 は、通信部 6 1 を介して、サービスプロバイダ 3 の相互認証部 4 5 と相互認証し、相互認証できたとき、通信部 6 1 は、相互認証したサービスプロバイダ 3 から、サービスプロバイダセキュアコンテナを受信する。相互認証できなかった場合、処理は終了されるが、この例の場合、相互認証されたものとし、ステップ S 2 4 2 に進む。

## 【0187】

ステップ S 2 4 2 において、レシーバ 5 1 の通信部 6 1 は、ステップ S 2 4 1 で相互認証したサービスプロバイダ 3 から、公開鍵証明書を受信する。

## 【0188】

ステップ S 2 4 3 において、レシーバ 5 1 の復号／暗号化モジュール 7 4 は、ステップ S 2 4 1 で受信したサービスプロバイダセキュアコンテナに含まれる署名を検証し、改竄がなかったか否かを検証する。ここで、改竄が発見された場合、処理は終了するが、この例の場合、改竄が発見されなかったものとし、ステップ S 2 4 4 に進む。

## 【0189】

ステップ S 2 4 4 において、レシーバ 5 1 の記憶モジュール 7 3 に記憶されている基準情報 5 1 が、利用条件を満たす UCP と価格条件を満たす PT が選択され、表示制御部 6 7 を介して、図示せず表示部に表示される。ユーザは、表示された UCP および PT の内容を参照して、図示せぬ操作部を操作し、UCP の 1 つの利用内容を選択する。これにより、入力制御部 6 8 は、操作部から入力された、ユーザの操作に対応する信号を SAM 6 2 に出力する。

## 【0190】

この例の場合、基準情報 5 1 の「利用ポイント情報」には、200 ポイント以上の利用ポイントが設定されているものとされているので、UCPA が選択可能となり、また基準情報 5 1 の「決済ユーザ情報」には、ユーザは男性とされているので、PTA-1 の「価格条件 10」に設定された条件を満たす。そこで、この例

の場合、UCPAに対応して作成されたPTA-1、PTA-2のうち、PTA-1が選択され、UCPAおよびPTA-1の内容が、表示部に表示される。また、この例の場合、そこで、ユーザは、UCPAの利用内容13（PTA-1の価格内容13）を選択したものとする。

【0191】

ステップS245において、レシーバ51のSAM62の課金処理モジュール72は、ステップS244で選択された、UCPAの「利用内容13」の内容（PTA-1の「価格内容13」の内容）に基づいて、UCSAおよび課金情報Aを作成する。

【0192】

ステップS246において、サービスプロバイダセキュアコンテナに含まれる、コンテンツA（コンテンツ鍵Kc o Aで暗号化されている）、UCPA、PTA-1、PTA-2、およびコンテンツプロバイダ2の署名は取り出され、HDD52に出力され、記憶される。ステップS247において、復号／暗号化ユニット74の復号ユニット91は、サービスプロバイダセキュアコンテナに含まれるコンテンツ鍵Kc o A（配送用鍵Kdで暗号化されている）を、記憶モジュール73に記憶されている配送用鍵Kdで復号する。

【0193】

ステップS248において、復号／暗号化ユニット74の暗号化ユニット93は、ステップS247で復号されたコンテンツ鍵Kc o Aを、記憶モジュール73に記憶されている保存用鍵K s a v eで暗号化する。

【0194】

ステップS249において、SAM62のデータ検査モジュール75は、ステップS248で保存用鍵K s a v eで暗号化されたコンテンツ鍵Kc o A、およびステップS245で作成されたUCSAが対応して記憶される、外部記憶部63の利用情報記憶部63AのブロックBPを検出する。この例の場合、利用情報記憶部63AのブロックBP-1が検出される。なお、図22の利用情報記憶部63Aにおいて、そのブロックBP-1の利用情報用メモリ領域RP-3にコンテンツ鍵Kc o AおよびUCSAが、すでに記憶されているように示されているが、この

例の場合、この時点において、それらは記憶されておらず、ブロックBP-1の利用情報用メモリ領域RP-3は、空いており、所定の初期情報が記憶されているものとする。

## 【0195】

ステップS250において、レシーバ51のデータ検査モジュール75は、ステップS249で検出したブロックBP-1のデータ（利用情報用メモリ領域RP-1乃至RP-Nに記憶されている全てのデータ）にハッシュ関数を適用してハッシュ値を得る。次に、ステップS251において、データ検査モジュール75は、ステップS250で得られたハッシュ値と、記憶モジュール73に記憶されているブロックBP-1に対応する検査値HP-1とを比較し、値が一致するか否かを判定し、一致すると判定した場合、そのブロックBP-1のデータは改竄されていないので、ステップS252に進む。

## 【0196】

ステップS252において、レシーバ51のSAM62は、利用情報（ステップS248で、保存用鍵Ksaveで暗号化されたコンテンツ鍵KcoA、およびステップS245で作成されたUCSA）を、利用情報記憶部63A（外部記憶部63）のブロックBP-1の利用情報用メモリ領域RP-3に記憶させる。

## 【0197】

ステップS253において、レシーバ51のデータ検査モジュール75は、ステップS252で利用情報が記憶された利用情報用メモリ領域RP-3が属する、利用情報記憶部63AのブロックBP-1のデータにハッシュ関数を適用してハッシュ値を算出し、ステップS254において、記憶モジュール73に記憶されている検査値HP-1に上書きする。ステップS255において、課金処理モジュール72は、ステップS245で作成した課金情報Aを記憶モジュール73に記憶させ、処理は終了する。

## 【0198】

ステップS251において、算出されたハッシュ値と検査値HP-1とが一致しないと判定された場合、ブロックBP-1のデータは改竄されているので、手続きは、ステップS256に進み、データ検査モジュール75は、外部記憶部6

3の利用情報記憶部63Aの全てのブロックBPを調べたか否かを判定し、外部記憶部63の全てのブロックBPを調べていないと判定した場合、ステップS257に進み、利用情報記憶部63Aの、調べていない（空きを有する他の）ブロックBPを検索し、ステップS250に戻り、それ以降の処理が実行される。

【0199】

ステップS256において、外部記憶部63の利用情報記憶部63Aの全てのブロックBPが調べられたと判定された場合、利用情報を記憶できるブロックBP（利用情報用メモリ領域RP）は存在しないので、処理は終了する。

【0200】

このように、サービスプロバイダセキュアコンテナが、レシーバ51により受信されると、処理は終了し、図33のステップS15に進む。

【0201】

ステップS15において、供給されたコンテンツAが、レシーバ51において利用される。なお、この例の場合、図40のステップS224で選択されたUCPAの利用内容13によれば、コンテンツAは、再生して利用される。そこで、ここでは、コンテンツAの再生処理について説明する。この再生処理の詳細は、図41のフローチャートに示されている。

【0202】

ステップS261において、レシーバ51のデータ検査モジュール75は、図40のステップS252で、コンテンツ鍵KcoA（保存用鍵Ksaveで暗号化されている）およびUCSAが記憶された利用情報用メモリ領域RP-3が属する、外部記憶部63の利用情報記憶部63AのブロックBP-1のデータにハッシュ関数を適用してハッシュ値を算出する。

【0203】

ステップS262において、レシーバ51のデータ検査モジュール75は、ステップS261において算出したハッシュ値が、図40のステップS253で算出し、ステップS254で記憶モジュール73に記憶させたハッシュ値（検査値HP-1）と一致するか否かを判定し、一致すると判定した場合、ブロックBP-1のデータは改竄されていないので、ステップS263に進む。

## 【0204】

ステップS263において、UCSA（図21）の「利用内容」の「パラメータ」に示されている情報に基づいて、コンテンツAが利用可能か否かが判定される。例えば、「利用内容」の「形式」が、「期間制限再生」とされているUCSにおいては、その「パラメータ」には、その開始期間（時刻）と終了期間（時刻）が記憶されているので、この場合、現在の時刻が、その範囲内にあるか否かが判定される。すなわち、現在時刻が、その範囲内にあるとき、そのコンテンツの利用が可能であると判定され、範囲外にあるとき、利用不可と判定される。また、「利用内容」の「形式」が、所定の回数に限って再生（複製）する利用形式とされているUCSにおいては、その「パラメータ」には、残された利用可能回数が記憶されている。この場合、「パラメータ」に記憶されている利用可能回数が0回でないとき、対応するコンテンツの利用が可能であると判定され、利用可能回数が0回であるとき、利用不可と判定される。

## 【0205】

なお、UCSAの「利用内容」の「形式」は、「期間制限再生」とされているが、この場合、現在の時刻が、その期間内であるとし、ステップS263において、コンテンツAが利用可能であると判定され、ステップS264に進む。

## 【0206】

ステップS264において、レシーバ51の課金モジュール72は、UCSAを更新する。UCSAには、更新すべき情報は含まれていないが、例えば、「利用内容」の「形式」が所定の回数に限って再生する利用形式とされている場合、その「パラメータ」に記憶されている、再生可能回数が1つだけデクリメントされる。

## 【0207】

次に、ステップS265において、レシーバ51のSAM62は、ステップS264で更新されたUCSA（実際は、更新されていない）を、外部記憶部63の利用情報記憶部63AのブロックBP-1の利用情報用メモリ領域RP-3に記憶させる。ステップS266において、データ検査モジュール75は、ステップS265でUCSAが記憶された、外部記憶部63の利用情報記憶部63Aのブロック

BP-1 のデータにハッシュ関数を適用して、ハッシュ値を算出し、記憶モジュール 73 に記憶されている検査値 HP-1 に上書きする。

【0208】

ステップ S267 において、SAM62 の相互認証モジュール 71 と、伸張部 64 の相互認証モジュール 101 は、相互認証し、SAM62 および伸張部 64 は、一時鍵 Ktemp を共有する。この認証処理は、図 35 乃至図 37 を参照して説明した場合と同様であるので、ここでは説明を省略する。相互認証に用いられる乱数 R1、R2、R3、またはその組み合わせが、一時鍵 Ktemp として用いられる。

【0209】

ステップ S268 において、復号／暗号化モジュール 74 の復号ユニット 91 は、図 40 のステップ S252 で外部記憶部 63 の利用情報記憶部 63A のブロック BP-1（利用情報用メモリ領域 RP-3）に記憶されたコンテンツ鍵 KcoA（保存用鍵 Ksave で暗号化されている）を、記憶モジュール 73 に記憶された保存用鍵 Ksave で復号する。

【0210】

次に、ステップ S269 において、復号／暗号化モジュール 74 の暗号化ユニット 93 は、復号されたコンテンツ鍵 KcoA を一時鍵 Ktemp で暗号化する。ステップ S270 において、SAM62 は、一時鍵 Ktemp で暗号化されたコンテンツ鍵 KcoA を伸張部 64 に送信する。

【0211】

ステップ S271 において、伸張部 64 の復号モジュール 102 は、コンテンツ鍵 KcoA を一時鍵 Ktemp で復号する。ステップ S272 において、伸張部 64 は、インタフェース 66 を介して、HDD52 に記録されたコンテンツ A（コンテンツ鍵 Kco で暗号化されている）を受け取る。ステップ S273 において、伸張部 64 の復号モジュール 103 は、コンテンツ A（コンテンツ鍵 Kco で暗号化されている）をコンテンツ鍵 KcoA で復号する。

【0212】

ステップ S274 において、伸張部 64 の伸張モジュール 104 は、復号され

たコンテンツ A を ATRAC2 などの所定の方式で伸張する。ステップ S 275 において、伸張部 64 のウォーターマーク付加モジュール 105 は、伸張されたコンテンツ A にレシーバ 51 を特定する所定のウォーターマーク（電子透かし）を挿入する。ステップ S 276 において、コンテンツ A は、図示せぬスピーカなどに出力され、処理は終了する。

#### 【0213】

ステップ S 262 において、ステップ S 261 において算出されたハッシュ値が、レシーバ 51 の記憶モジュール 73 に記憶されたハッシュ値と一致しないと判定された場合、またはステップ S 263 において、コンテンツが利用不可と判定された場合、ステップ S 277 において、SAM 62 は、表示制御部 67 を介して、図示せぬ表示部にエラーメッセージを表示させる等の所定のエラー処理を実行し、処理は終了する。

#### 【0214】

このようにして、レシーバ 51 において、コンテンツ A が再生（利用）されたとき、処理は終了し、図 33 の処理も終了する。

#### 【0215】

次に、レシーバ 51 において計上された課金を決済する場合の処理手順を、図 42 のフローチャートを参照して説明する。なお、この処理は、計上された課金が所定の上限額（正式登録時の上限額または仮登録時の上限額）を越えた場合、または配送用鍵 K d のバージョンが古くなり、例えば、図 40 のステップ S 247 で、コンテンツ鍵 K c o（配送用鍵 K d で暗号化されている）を復号することができなくなった場合（サービスプロバイダセキュアコンテナを受信することができなくなった場合）に開始される。

#### 【0216】

ステップ S 301 において、レシーバ 51 と EMD サービスセンタ 1 との相互認証が行われる。この相互認証は、図 35 乃至図 37 を参照して説明した場合と同様の処理であるので、その説明は省略する。

#### 【0217】

次に、ステップ S 302 において、レシーバ 51 の SAM 62 は、EMD サービスセ

ンタ 1 のユーザ管理部 18 (図 3) に証明書を送信する。ステップ S 3 0 3 において、レシーバ 5 1 の SAM 6 2 は、決済される課金 (課金情報) に対応する UCP を、ステップ S 3 0 1 で EMD サービスセンタ 1 と共有した一時鍵  $K_{temp}$  で暗号化し、記憶モジュール 7 3 に記憶されている、配送用鍵  $K_d$  のバージョン、課金情報 (例えば、図 2 3 の課金情報 A)、および登録リストとともに、EMD サービスセンタ 1 に送信する。

#### 【0218】

ステップ S 3 0 4 において、EMD サービスセンタ 1 のユーザ管理部 18 は、ステップ S 3 0 3 で、レシーバ 5 1 から送信された情報を受信し、復号した後、EMD サービスセンタ 1 のユーザ管理部 18 が、登録リストの「状態フラグ」に”停止”が設定されるべき不正行為がレシーバ 5 1 において存在するか否かを確認する。

#### 【0219】

ステップ S 3 0 5 において、EMD サービスセンタ 1 の課金請求部 19 は、ステップ S 3 0 3 で受信された課金情報を解析し、ユーザの支払い金額を算出する処理等を行う。次に、ステップ S 3 0 6 において、ユーザ管理部 18 は、ステップ S 3 0 5 における処理により、決済が成功したか否かを確認する。

#### 【0220】

次に、ステップ S 3 0 7 において、EMD サービスセンタ 1 のユーザ管理部 18 は、ステップ S 3 0 4 における確認結果、およびステップ S 3 0 6 における確認結果に基づいて、レシーバ 5 1 の登録条件を設定し、それに署名を付して、レシーバ 5 1 の登録リストを作成する。

#### 【0221】

例えば、ステップ S 3 0 4 で、不正行為が確認された場合、「状態フラグ」には”停止”が設定され、この場合、今後、全ての処理が停止される。すなわち、EMD システムからのサービスを一切受けることができなくなる。また、ステップ S 3 0 6 で、決済が成功しなかったことが確認された場合、「状態フラグ」には”制限あり”が設定され、この場合、すでに購入したコンテンツを再生する処理は可能とされるが、新たにコンテンツを購入する処理は実行できなくなる。



## 【0222】

次に、ステップS308に進み、EMDサービスセンタ1のユーザ管理部18は、最新バージョンの配送用鍵Kd（3月分の最新バージョンの配送用鍵Kd）およびステップS307で作成された登録リストを、一時鍵Ktempで暗号化し、レシーバ51に送信する。

## 【0223】

ステップS309において、レシーバ51のSAM62は、EMDサービスセンタ1から送信された配送用鍵Kdおよび登録リストを、通信部61を介して受信し、復号した後、記憶モジュール73に記憶させる。このとき、記憶モジュール73に記憶されていた課金情報は消去され、登録リストおよび配送用鍵Kdが更新される。また、このとき、受信された登録リストの登録リスト署名が検証され、登録リストが改竄されていないとが確認される。この署名の確認処理は、図37のステップS83における処理と同様であるので、その説明は省略する。

## 【0224】

次に、コンテンツを利用する権利を再購入する場合のレシーバ51の処理手順を、図43のフローチャートを参照して説明する。ここでは、コンテンツAを”期間制限再生”の利用形式で利用することができる権利を保持している（すでに購入している）レシーバ51が、”買い取り再生”の利用形式で利用する権利を購入する場合を例として説明する。

## 【0225】

ステップS401において、HDD52に記憶されているコンテンツA、UCPA、およびPTA-1、A-2が改竄されているか否かが判定される。具体的には、レシーバ51の復号/暗号化モジュール74が、図40のステップS246で、コンテンツA、UCPA、およびPTA-1、A-2とともに、HDD52に記憶させた署名を、公開鍵暗号の公開鍵で復号し、その結果（ハッシュ値）と、コンテンツA、UCPA、およびPTA-1、A-2の全体のハッシュ値とが、等しいか否かを判定する。それらの値が等しいと判定された場合、データは、改竄されていないと判定され、ステップS402に進む。

## 【0226】

ステップS402において、コンテンツAに対応する利用情報（コンテンツ鍵KcoAおよびUCSA）が改竄されているか否かが判定される。具体的には、レシーバ51のデータ検査モジュール75が、コンテンツAの利用情報が記憶されている、外部記憶部63の利用情報記憶部63AのブロックBP（この例の場合、ブロックBP-1）のデータにハッシュ関数を適用してハッシュ値を算出し、それが、記憶モジュール73に記憶されている、そのブロックBPに対応する検査値HP（この例の場合、検査値HP-1）と等しいか否かを判定する。それらの値が等しいと判定された場合、利用情報が改竄されていないと判定され、ステップS403に進み、レシーバ51のSAM62は、外部記憶部63の利用情報記憶部63Aから、UCSAを取り出す。

## 【0227】

次に、ステップS404において、SAM62は、UCSと課金情報を作成する。具体的には、表示制御部67が、UCPA、PTA-1、A-2、およびUCSAの内容を、図示せぬ表示部に表示する。そこで、ユーザFは、UCSAの「利用内容」の「形式」に、“期限制限再生”（形式13）が設定されていることから、UCPAの「利用内容15」の「形式15」での利用が可能であること、その価格（PTA-1の価格内容15）などを確認する。そして、この例の場合、ユーザFは、UCPAの「利用内容15」およびPTA-1を選択する操作を、レシーバ51の図示せぬ操作部に対して行う。これにより、入力制御部68は、ユーザの操作に対応する信号（UCPAの「利用内容15」のIDとPTA-1のID）を操作部から受信し、それをSAM62に出力する。その後、SAM62の課金モジュール72は、入力制御部68からのUCPAの「利用内容15」のIDとPTA-1のIDに基づいて、図44および図45に示すように、「利用内容」のUCPAの「利用形式15」の内容が設定されたUCSBおよび課金情報Bを作成する。

## 【0228】

次に、ステップS405において、レシーバ51のSAM62は、ステップS404で作成された課金情報Bを、記憶モジュール73に記憶させ、ステップS406において、ステップS404で作成されたUCSBを、UCSAに換えて外部記憶部63の利用情報記憶部63Aに記憶させる。

## 【0229】

ステップS407において、レシーバ51のデータ検査モジュール75は、ステップS406で、UCSBが記憶された、外部記憶部63の利用情報記憶部63AのブロックBPのデータにハッシュ関数を適用してハッシュ値を算出する。そして、ステップS408において、データ検査モジュール75は、算出したハッシュ値を記憶モジュール73に記憶されている、そのブロックBPに対応する検査値HPに上書きする。その後、処理は終了される。

## 【0230】

ステップS401において、コンテンツA、UCPA、およびPTA-1、A-2が改竄されていると判定された場合、またはステップS402において、コンテンツ鍵Kc o AおよびUCSAが改竄されていると判定された場合、処理は終了する。

## 【0231】

以上のようにして、レシーバ51は、コンテンツAを利用する権利の再購入する。

## 【0232】

なお、ステップS403で作成された課金情報Bに基づいて計上された課金は、図42のフローチャートで説明した決済処理により決済される。すなわち、この例の場合、ユーザは、コンテンツAを、新規に購入する場合の買い取り価格（2000円）比べ、割安の価格（1980円）で購入することができる。

## 【0233】

次に、レシーバ301において権利を再購入する場合の処理手順を、図46のフローチャートを参照して説明する。レシーバ51が、図43のフローチャートで説明した処理により、コンテンツAをレシーバ51において”買い取り再生”の利用形式で利用する権利を有している状態で、さらにコンテンツAをレシーバ301において”買い取り再生”で利用する権利を購入する場合を例として説明する。

## 【0234】

ステップS421において、レシーバ51（コンテンツを供給する機器）のSA

M62およびレシーバ301（コンテンツの供給を受ける機器）のSAM311のそれぞれは、各自が保持する登録リストの登録条件を参照し、再購入処理の実行が可能であるか否かを確認する。具体的には、コンテンツの供給機器のSAM（この例の場合、レシーバ51のSAM62）は、自分の登録リストに、コンテンツの供給を受ける機器（この例の場合、レシーバ301）の登録条件が設定されており、またその「コンテンツ供給機器」に自分自身のSAMのIDが設定されているか否かを確認する。コンテンツの供給を受ける機器は、登録リストの自分自身の登録条件の「コンテンツ供給機器」に、コンテンツを供給する機器が設定されているか否かを確認する。

#### 【0235】

この例の場合、ここでは、レシーバ51において、レシーバ51の登録リストに、レシーバ301の登録リストが設定され、かつその「コンテンツ供給機器」にSAM62のIDが設定され、そしてレシーバ301において、レシーバ301の登録リストのレシーバ301の登録条件の「コンテンツ供給機器」にSAM62のIDが設定されているので、再購入処理の実行が可能であることが確認され、ステップS422に進む。

#### 【0236】

ステップS422において、レシーバ51とレシーバ301との相互認証が行われる。この相互認証は、図37を参照して説明した場合と同様であるので、その説明は省略するが、これにより、レシーバ51とレシーバ301は、一時鍵Ktempを共有する。

#### 【0237】

ステップS423において、レシーバ51は、HDD52に記憶されているコンテンツA、UCPA、およびPTA-1、A-2が改竄されているか否かを判定する。具体的には、レシーバ51の復号/暗号化モジュール74が、図40のステップS246で、コンテンツA、UCPA、およびPTA-1、A-2とともに、HDD52に記憶された署名を、公開鍵暗号の公開鍵で復号し、その結果（ハッシュ値）と、コンテンツA、UCPA、およびPTA-1、A-2の全体のハッシュ値とが、等しいか否かを判定する。それらの値が等しいと判定された場合、データは改竄

されていないと判定され、ステップS424に進む。

【0238】

ステップS424において、レシーバ51は、コンテンツAに対応する利用情報（コンテンツ鍵Kc o AおよびUCSB）が改竄されているか否かを判定する。具体的には、レシーバ51のデータ検査モジュール75が、コンテンツAの利用情報が記憶されている、外部記憶部63の利用情報記憶部63AのブロックBP（この例の場合、ブロックBP-1）のデータにハッシュ関数を適用してハッシュ値を算出し、それが、記憶モジュール73に記憶されている、そのブロックBPに対応する検査値HP（この例の場合、検査値HP-1）と等しいか否かを判定する。それらの値が等しいと判定された場合、利用情報が改竄されていないと判定され、ステップS425に進む。

【0239】

ステップS425において、レシーバ51は、UCSと課金情報を作成する。具体的には、表示制御部67は、UCPA、PTA-1、A-2、およびUCSBの内容を、図示せぬ表示部に表示する。そこで、ユーザF（または、ユーザA）は、UCSBの「利用内容」の「形式」に、“形式13→形式11”が設定されていることから（現在、コンテンツAを“買い取り再生”で利用する権利を有していることから）、UCPAの「利用内容16」の「形式16」での利用が可能であること、その価格（PTA-1の価格内容16）などを確認する。そして、この例の場合、ユーザFは、UCPAの「利用内容16」およびPTA-1を選択する操作を、図示せぬ操作部に対して行う。これにより、入力制御部68は、ユーザFの操作に対応する信号（UCPAの「利用内容16」のIDとPTA-1のID）を操作部から受信し、それをSAM62に出力する。その後、SAM62の課金モジュール72は、入力制御部68からのUCPAの「利用内容16」のIDとPTA-1のIDに基づいて、図47および図48に示すように、「利用内容」にUCPAの「利用内容16」の内容が設定されたUCSCおよび課金情報Cを作成する。

【0240】

次に、ステップS426において、HDD52に記憶されている、コンテンツA、UCPA、およびPTA-1、A-2、ステップS423で、改竄されていないこ

とが確認されたコンテンツ鍵K c o A、ステップS 4 2 5で作成されたUCSB、および署名（UCSBおよびコンテンツ鍵K c o Aに対する署名）が、レシーバ3 0 1に送信される。なお、UCSB、コンテンツ鍵K c o A、および署名は、SAM 6 2が、一時鍵K t e m pで暗号化し、通信部6 5を介して、レシーバ3 0 1に送信する。また、UCSBは、レシーバ3 0 1に送信された後、権利の増殖を防止するために消去される。

#### 【0 2 4 1】

コンテンツの供給を受ける機器であるレシーバ3 0 1は、上述したように、UC P、PT、およびUCSの内容をユーザに表示する表示部や、利用内容等を選択することができる操作部を有しておらず、そのため、UCSや課金情報を自分自身で作成することができない。そこで、このような場合、ステップS 4 2 5において、コンテンツを供給する機器であるレシーバ5 1により、UCSおよび課金情報が作成される。また、レシーバ3 0 1は、上述したように、課金処理を実行することができないので、作成された課金情報は、ステップS 4 2 6で、レシーバ3 0 1に送信されず、レシーバ5 1により保持され、レシーバ5 1により処理される。

#### 【0 2 4 2】

次に、ステップS 4 2 7において、レシーバ3 0 1のSAM 3 1 1は、ステップS 4 2 6で、レシーバ5 1から送信されてきたデータを受信する。なお、一時鍵K t e m pで暗号化されて送信されてきたUCSB、コンテンツ鍵K c o A、および署名は、一時鍵K t e m pで復号される。

#### 【0 2 4 3】

ステップS 4 2 8において、レシーバ3 0 1の復号／暗号化モジュール3 2 4は、ステップS 4 2 7で受信されたUCSBおよびコンテンツ鍵K c o Aに付された署名を確認し、UCSBおよびコンテンツ鍵K c o Aが改竄が改竄されているか否かを判定する。この署名の確認は、図3 7のステップS 8 3における処理と同様であるので、その説明は省略する。

#### 【0 2 4 4】

ステップS 4 2 8において、UCSBおよびコンテンツ鍵K c o Aが改竄されていないと判定された場合、ステップS 4 2 9に進み、レシーバ3 0 1のSAM 3 1

1 は、ステップ S 4 2 7 で受信されたコンテンツ A、UCPA、および PTA-1、PTA-2 を記憶モジュール 3 2 3 に記憶させる。

【0245】

ステップ S 4 3 0 において、レシーバ 3 0 1 のデータ検査モジュール 3 2 5 は、コンテンツ鍵 K c o A を記憶する、外部記憶部 3 1 2 の利用情報記憶部 3 1 2 A のブロック BP を検出する。次に、ステップ S 4 3 1 において、レシーバ 3 0 1 のデータ検査モジュール 3 2 5 は、ステップ S 4 3 0 で検出した、利用情報記憶部 3 1 2 A のブロック BP のデータにハッシュ関数を適用してハッシュ値を算出し、記憶モジュール 3 2 3 に記憶されている、検出されたブロック BP に対応する検査値 HP と一致しているか否かを判定する。それらの値が一致すると判定された場合、すなわち、ステップ S 4 3 0 で検出されたブロック BP が改竄されていない場合、ステップ S 4 3 2 に進み、データ検査モジュール 3 2 5 は、ステップ S 4 2 7 で受信された UCSB およびコンテンツ鍵 K c o A を、それぞれ対応させてブロック BP に記憶させる。

【0246】

ステップ S 4 3 3 において、レシーバ 3 0 1 のデータ検査モジュール 3 2 5 は、ステップ S 4 3 2 で、UCSB およびコンテンツ鍵 K c o A が記憶された外部記憶部 3 1 2 の利用情報記憶部 3 1 2 A のブロック BP のデータにハッシュ関数を適用してハッシュ値を算出し、記憶モジュール 3 2 3 に記憶されている、そのブロック BP に対応する検査値 HP に上書きする。その後、処理は終了される。

【0247】

ステップ S 4 2 8 において、レシーバ 5 1 からのデータが改竄されていると判定された場合、ステップ S 4 3 4 に進み、レシーバ 3 0 1 の SAM 3 1 1 は、その旨をレシーバ 5 1 に通知する等の処理を実行する。その後、ステップ S 4 2 4 に戻る。すなわち、これにより、コンテンツ A、UCPA、PTA-1、A-2、UCSB、コンテンツ鍵 K c o A、および署名が、再度、レシーバ 3 0 1 に送信される。なお、この例の場合、レシーバ 5 1 からのこの送信は、予め決められた回数だけ行われるものとし、その回数を越えた場合、処理は終了されるものとする。

【0248】

ステップ S 4 2 1 で、再購入処理の実行が可能でないと判定された場合、ステップ S 4 2 3 で、コンテンツ A、UCPA、および PTA-1, A-2 が改竄されていると判定された場合、ステップ S 4 2 4 で、UCSB および コンテンツ鍵 K c o A が改竄されていると判定された場合、またはステップ S 4 3 1 において、検出されたブロック BP が改竄されていると判定された場合、処理は終了される。

#### 【0249】

次に、レシーバ 201 において権利を再購入する場合の処理手順を、図 49 のフローチャートを参照して説明する。レシーバ 51 が、図 43 のフローチャートで説明した処理により、コンテンツ A をレシーバ 51 において”買い取り再生”の利用形式で利用する権利を有している状態で、さらにコンテンツ A をレシーバ 201 において”買い取り再生”で利用する権利を購入する場合を例として説明する。

#### 【0250】

ステップ S 4 5 1 において、レシーバ 51 の SAM 6 2 および レシーバ 201 の SAM 2 1 2 のそれぞれは、各自が保持する登録リストの登録条件を参照し、再購入処理の実行が可能か否かを確認する。なお、ここでの具体的な処理は、図 46 のステップ S 4 2 1 における場合と同様であるので、その説明は省略するが、この例の場合、再購入処理の実行が可能であると判定され、ステップ S 4 5 2 に進む。

#### 【0251】

ステップ S 4 5 2 において、レシーバ 51 と レシーバ 201 との相互認証が行われる。この相互認証は、図 37 を参照して説明した場合と同様であるので、その説明は省略するが、これにより、レシーバ 51 と レシーバ 201 は、一時鍵 K t e m p を共有する。

#### 【0252】

ステップ S 4 5 3 において、コンテンツ A に対応する利用情報（コンテンツ鍵 K c o A および UCSB）が改竄されているか否かが判定される。具体的には、レシーバ 51 のデータ検査モジュール 75 が、コンテンツ A の利用情報が記憶されている、外部記憶部 63 の利用情報記憶部 63 A のブロック BP（この例の場合



、ブロックBP-1)のデータにハッシュ関数を適用してハッシュ値を算出し、それが、記憶モジュール73に記憶されている、そのブロックBPに対応する検査値HP(この例の場合、検査値HP-1)と等しいか否かを判定する。それらの値が等しいと判定された場合、利用情報が改竄されていないと判定され、ステップS454に進む。

#### 【0253】

ステップS454において、図40のステップS246で、レシーバ201のHDD52に記憶された、コンテンツA、UCPA、PTA-1、A-2、および署名(コンテンツA、UCPA、PTA-1、PTA-2に対する署名)、並びに、ステップS453で、改竄されていないことが確認された、UCSB、コンテンツ鍵KcoA、および署名(UCSBおよびコンテンツ鍵KcoAに対する署名)が、レシーバ201に送信される。なお、UCSB、コンテンツ鍵KcoA、および署名は、SAM62が、一時鍵Ktempで暗号化し、通信部65を介して、レシーバ201に送信する。

#### 【0254】

次に、ステップS455において、レシーバ201のSAM212は、ステップS454で、レシーバ51から送信されてきたデータを受信する。なお、一時鍵Ktempで暗号化されて送信されてきたUCSB、コンテンツ鍵KcoA、および署名は、一時鍵Ktempで復号される。

#### 【0255】

ステップS456において、レシーバ201の復号/暗号化モジュール224は、ステップS455で受信されたUCSBおよびコンテンツ鍵KcoAの署名を確認し、UCSBおよびコンテンツ鍵KcoAが改竄が改竄されているか否かを判定し、改竄されていないと判定した場合、ステップS457に進む。この署名の確認は、図37のステップS83における処理と同様であるので、その説明は省略する。

#### 【0256】

ステップS457において、レシーバ201の復号/暗号化モジュール224は、ステップS455で受信されたコンテンツA、UCPA、およびPTA-1、A

ー 2 が改竄されているか否かを判定する。具体的には、レシーバ 201 の復号／暗号化モジュール 224 が、ステップ S455 で受信された署名（コンテンツ A、UCPA、および PTA-1、A-2 に対する署名）を、公開鍵暗号の公開鍵で復号し、その結果（ハッシュ値）と、コンテンツ A、UCPA、および PTA-1、A-2 の全体のハッシュ値とが等しいか否かを判定する。それらの値が等しいと判定された場合、データは改竄されていないと判定され、ステップ S458 に進む。

#### 【0257】

ステップ S458 において、レシーバ 201 の SAM 212 は、ステップ S455 で受信されたコンテンツ A、UCPA、および PTA-1、PTA-2 を、自分自身の署名を付して、HDD 202 に記憶させる。

#### 【0258】

ステップ S459 において、レシーバ 201 のデータ検査モジュール 225 は、コンテンツ鍵 Kc o A を記憶する、外部記憶部 213 の利用情報記憶部 213 A のブロック BP を検出する。ステップ S460 において、レシーバ 201 のデータ検査モジュール 225 は、ステップ S459 で検出した、利用情報記憶部 213 A のブロック BP のデータにハッシュ関数を適用してハッシュ値を算出し、記憶モジュール 223 に記憶されている、検出されたブロック BP に対応する検査値 HP と一致しているか否かを判定する。それらの値が一致すると判定された場合、すなわち、ステップ S459 で検出されたブロック BP が改竄されていない場合、ステップ S461 に進む。

#### 【0259】

ステップ S461 において、レシーバ 201 の SAM 212 は、UCS と課金情報を作成する。具体的には、表示制御部 217 は、UCPA、PTA-1、A-2、および UCSB の内容を、図示せぬ表示部に表示する。そこで、ユーザ F（または、ユーザ A）は、UCSB の「利用内容」の「形式」に、“形式 13 → 形式 11” が設定されていることから（現在、コンテンツ A を“買い取り再生”で利用する権利を有していることから）、UCPA の「利用内容 16」の「形式 16」での利用が可能であること、その価格（PTA-1 の価格内容 16）などを確認する。そし

て、この例の場合、ユーザFは、UCPAの「利用内容16」およびPTA-1を選択する操作を、レシーバ201の図示せぬ操作部に対して行う。これにより、入力制御部218は、ユーザFの操作に対応する信号（UCPAの「利用内容16」のIDとPTA-1のID）を操作部から受信し、それをSAM212に出力する。その後、SAM212の課金モジュール222は、入力制御部218からのUCPAの「利用内容16」のIDとPTA-1のIDに基づいて、図50および図51に示すように、「利用内容」にUCPAの「利用内容16」に内容が設定されたUCSDおよび課金情報Dを作成する。なお、UCSDが作成された後、レシーバ51から供給されたUCSBは、権利の増殖を防止するために消去される。

#### 【0260】

次に、ステップS462において、レシーバ201のSAM212は、ステップS461で作成された課金情報Dを、記憶モジュール223に記憶させる。

#### 【0261】

このように、レシーバ201は、表示部や操作部を有しているので、自分自身でUCSおよび課金情報を作成する。またレシーバ201は、課金処理を実行することができるので、作成した課金情報を保持し、所定のタイミングで、それを処理する。

#### 【0262】

ステップS463において、レシーバ201のSAM21は、ステップS461で作成されたUCSDを、コンテンツ鍵KcoAと対応させて、外部記憶部213の利用情報記憶部213Aの、ステップS459で検出されたブロックBPに記憶させる。

#### 【0263】

ステップS464において、レシーバ201のデータ検査モジュール225は、ステップS463で、UCSDおよびコンテンツ鍵KcoAが記憶された外部記憶部213の利用情報記憶部213AのブロックBPのデータにハッシュ関数を適用してハッシュ値を算出し、記憶モジュール223に記憶されている、そのブロックBPに対応する検査値HPに上書きする。その後、処理は終了される。

#### 【0264】

ステップS456において、レシーバ51からのデータが改竄されていると判定された場合、ステップS465に進み、レシーバ201のSAM212は、その旨をレシーバ51に通知する等の処理を実行する。その後、ステップS454に戻る。すなわち、これにより、コンテンツA、UCPA、PTA-1、A-2、UCSB、コンテンツ鍵KcoA、および署名が、再度、レシーバ201に送信される。なお、この例の場合、レシーバ51からのこの送信は、予め決められた回数だけ行われるものとし、その回数を越えた場合、処理は終了されるものとする。

#### 【0265】

ステップS451において、再購入処理の実行が可能でないと判定された場合、ステップS453において、UCSBおよびコンテンツ鍵KcoAが改竄されていると判定された場合、ステップS457において、コンテンツA、UCPA、およびPTA-1、A-2が改竄されていると判定された場合、またはステップS460において、検出されたブロックBPが改竄されていると判定された場合、処理は終了される。

#### 【0266】

以上においては、レシーバ51が、レシーバ201に供給する（ステップS454）場合と例として説明したが、レシーバ201は、それらを、別途（例えば、EMDサービスセンタ1から直接）取得するようにすることもできる。

#### 【0267】

また、以上においては、コンテンツを”期間制限再生”で利用する権利を有している状態において、”買い取り再生”で利用する権利を購入する場合、および”買い取り再生”で利用する権利を有している状態において、”買い取り再生”で利用する権利を再度（他の機器において）購入する場合を例として説明したが、その他利用形式の組み合わせにおいても、適用することができる。

#### 【0268】

また、以上においては、再購入の権利の内容を示す、UCPの「利用内容」（例えば、利用内容15または利用内容16）が選択された場合、UCSの「利用内容」の「ID」に「利用内容15」または「利用内容16」のIDが設定されるようにしたが、このとき再購入される「利用内容11」のIDが設定されるようにするこ

ともできる。

【0 2 6 9】

また、以上においては、SAMの、公開鍵K<sub>pu</sub>および証明書が、SAM内に（記憶モジュールに）記憶されるようにしたが、HDDに記憶させておくこともできる。

【0 2 7 0】

なお、コンテンツは、音楽データを例に説明したが、音楽データに限らず、動画像データ、静止画像データ、文書データ、またはプログラムデータでもよい。その際、圧縮は、コンテンツの種類に適した方式、例えば、画像であればMPEG(Moving Picture Experts Group)などが利用される。ウォーターマークも、コンテンツの種類に適した形式のウォーターマークが利用される。

【0 2 7 1】

また、共通鍵暗号は、ブロック暗号であるDESを使用して説明したが、NTT（商標）が提案するFEAL、IDEA(International Data Encryption Algorithm)、または1ビット乃至数ビット単位で暗号化するストリーム暗号などでもよい。

【0 2 7 2】

さらに、コンテンツおよびコンテンツ鍵K<sub>co</sub>の暗号化は、共通鍵暗号方式を利用するとして説明したが、公開鍵暗号方式でもよい。

【0 2 7 3】

なお、本明細書において、システムとは、複数の装置により構成される装置全体を表すものとする。

【0 2 7 4】

また、上記したような処理を行うコンピュータプログラムをユーザに提供する提供媒体としては、磁気ディスク、CD-ROM、固体メモリなどの記録媒体の他、ネットワーク、衛星などの通信媒体を利用することができる。

【0 2 7 5】

【発明の効果】

請求項1に記載の情報処理装置、請求項4に記載の情報処理方法、および請求項5に記載の提供媒体によれば、購入された権利の内容に基づいて再購入することができる権利の内容を示す第2の利用内容を含む取扱方針を記憶するようにし

たので、第2の利用内容、および第2の利用内容に対応する価格内容を特定する第2の使用許諾条件情報を作成することができる。

【0276】

請求項6に記載の情報処理装置、請求項7に記載の情報処理方法、および請求項8に記載の提供媒体によれば、使用許諾条件情報を受信するようにしたので、その使用許諾条件情報により特定される利用内容に示される権利の内容に基づいて、情報を利用することができる。

【0277】

請求項9に記載の情報処理装置、請求項10に記載の情報処理方法、および請求項11に記載の提供媒体によれば、権利の内容を示す第1の利用内容と、第1の利用内容に対応する価格内容を特定する使用許諾条件情報を作成するようにしたので、使用許諾条件情報を他の情報処理装置に送信することができる。

【0278】

請求項12に記載の情報処理装置、請求項14に記載の情報処理方法、および請求項15に記載の提供媒体によれば、他の情報処理装置から送信されてきた、使用許諾条件情報に含まれる利用内容により特定される権利の内容に基づいて再購入される第2の利用内容と、第2の利用内容に対応する価格内容を特定する第2の使用許諾条件情報を作成するようにしたので、第2の利用内容に示される権利の内容に基づいて、情報を利用することができる。

【図面の簡単な説明】

【図1】

EMDシステムを説明する図である。

【図2】

EMDシステムにおける、主な情報の流れを説明する図である。

【図3】

EMDサービスセンタ1の機能的構成を示すブロック図である。

【図4】

EMDサービスセンタ1の配送用鍵Kdの送信を説明する図である。

【図 5】

EMDサービスセンタ 1 の配送用鍵 K d の送信を説明する他の図である。

【図 6】

EMDサービスセンタ 1 の配送用鍵 K d の送信を説明する他の図である。

【図 7】

EMDサービスセンタ 1 の配送用鍵 K d の送信を説明する他の図である。

【図 8】

システム登録情報の例を説明する図である。

【図 9】

コンテンツプロバイダ 2 の機能的構成例を示すブロック図である。

【図 1 0】

UCPの例を示す図である。

【図 1 1】

コンテンツの管理移動を説明する図である。

【図 1 2】

第 1 世代複製を説明する図である。

【図 1 3】

コンテンツプロバイダセキュアコンテナの例を示す図である。

【図 1 4】

コンテンツプロバイダ 2 の証明書の例を示す図である。

【図 1 5】

サービスプロバイダ 3 の機能的構成を示すブロック図である。

【図 1 6】

PTの例を示す図である。

【図 1 7】

サービスプロバイダセキュアコンテナの例を示す図である。

【図 1 8】

サービスプロバイダ 3 の証明書の例を示す図である。

【図 1 9】

ユーザホームネットワーク 5 のレシーバ 5 1 の機能的構成例を示すブロック図である。

【図 2 0】

レシーバ 5 1 の SAM 6 2 の証明書の例を示す図である。

【図 2 1】

UCS の例を示す図である。

【図 2 2】

レシーバ 5 1 の外部記憶部 6 3 の利用情報記憶部 6 3 A の内部を説明する図である。

【図 2 3】

課金情報の例を示す図である。

【図 2 4】

レシーバ 5 1 の記憶モジュール 7 3 に記憶されている情報を示す図である。

【図 2 5】

基準情報 5 1 を説明する図である。

【図 2 6】

レシーバ 5 1 の登録リストの例を示す図である。

【図 2 7】

ユーザホームネットワーク 5 のレシーバ 2 0 1 の機能的構成例を示すブロック図である。

【図 2 8】

基準情報 5 1 を説明する図である。

【図 2 9】

レシーバ 2 0 1 の登録リストの例を示す図である。

【図 3 0】

ユーザホームネットワーク 5 のレシーバ 3 0 1 の機能的構成例を示すブロック図である。

【図 3 1】

基準情報 3 0 1 を説明する図である。



【図 3 2】

レシーバ 301 の登録リストの例を示す図である。

【図 3 3】

コンテンツの利用処理を説明するフローチャートである。

【図 3 4】

EMD サービスセンタ 1 がコンテンツプロバイダ 2 へ配送用鍵 K d を送信する処理を説明するフローチャートである。

【図 3 5】

コンテンツプロバイダ 2 と EMD サービスセンタ 1 との相互認証の動作を説明するフローチャートである。

【図 3 6】

コンテンツプロバイダ 2 と EMD サービスセンタ 1 との相互認証の他の動作を説明するフローチャートである。

【図 3 7】

コンテンツプロバイダ 2 と EMD サービスセンタ 1 との相互認証の他の動作を説明するフローチャートである。

【図 3 8】

コンテンツプロバイダ 2 がサービスプロバイダ 3 にコンテンツプロバイダセキュアコンテナを送信する処理を説明するフローチャートである。

【図 3 9】

サービスプロバイダ 3 がレシーバ 51 にサービスプロバイダセキュアコンテナを送信する処理を説明するフローチャートである。

【図 4 0】

レシーバ 51 がサービスプロバイダセキュアコンテナを受信する処理を説明するフローチャートである。

【図 4 1】

レシーバ 51 がコンテンツを再生する処理を説明するフローチャートである。

【図 4 2】

課金を決済する処理を説明するフローチャートである。

【図 4 3】

再購入処理を説明するフローチャートである。

【図 4 4】

他の UCS の例を示す図である。

【図 4 5】

他の課金情報の例を示す図である。

【図 4 6】

他の再購入処理を説明するフローチャートである。

【図 4 7】

他の UCS の例を示す図である。

【図 4 8】

他の課金情報の例を示す図である。

【図 4 9】

他の再購入処理を説明するフローチャートである。

【図 5 0】

他の UCS の例を示す図である。

【図 5 1】

他の課金情報の例を示す図である。

【符号の説明】

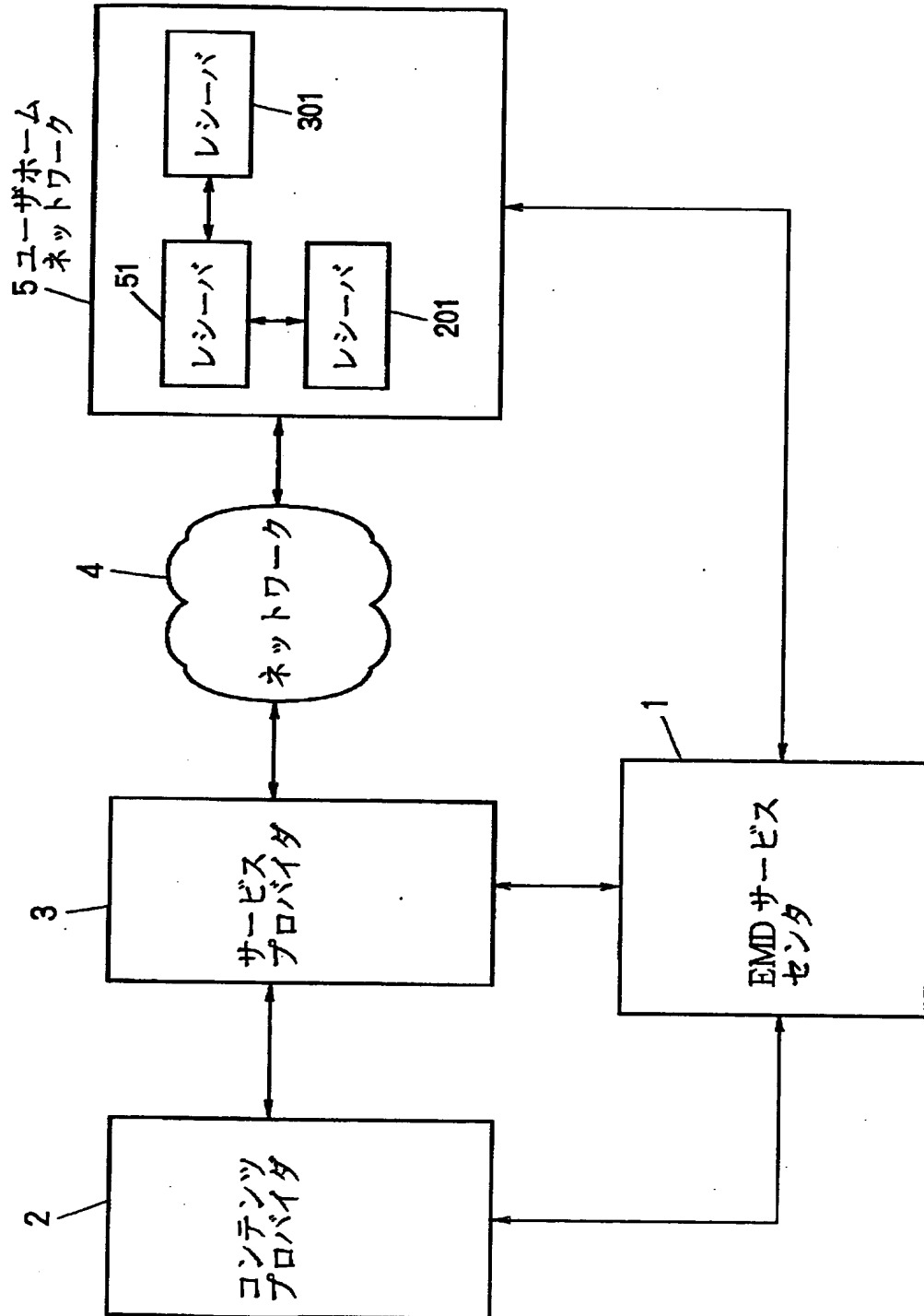
1 EMDサービスセンタ, 2 コンテンツプロバイダ, 3 サービスプロバイダ, 5 ユーザホームネットワーク, 11 サービスプロバイダ管理部, 12 コンテンツプロバイダ管理部, 13 著作権管理部, 14 鍵サーバ, 15 経歴データ管理部, 16 利益分配部, 17 相互認証部, 18 ユーザ管理部, 19 課金請求部, 20 出納部, 21 監査部, 31 コンテンツサーバ, 32 ウォータマーク付加部, 33 圧縮部, 34 暗号化部, 35 乱数発生部, 36 暗号化部, 37 ポリシー記憶部, 38 セキュアコンテナ作成部, 39 相互認証部, 41 コンテンツサーバ, 42 値付け部, 43 ポリシー記憶部, 44 セキュアコンテナ作成部, 45 相互認証部, 51 レシーバ, 52 HDD,

61 通信部, 62 SAM, 63 外部記憶部, 64 伸張部, 65  
 通信部, 66 インタフェース, 67 表示制御部, 68 入力制御部,  
 71 相互認証モジュール, 72 課金処理モジュール, 73 記憶モジ  
 ュール, 74 復号/暗号化モジュール, 75 データ検査モジュール,  
 91 復号ユニット, 92 乱数発生ユニット, 93 暗号化ユニット,  
 101 相互認証モジュール, 102 復号モジュール, 103 復号モジ  
 ュール, 104 伸張モジュール, 105 ウォータマーク付加モジュール  
 , 201 レシーバ, 202 HDD, 211 通信部, 212 SAM,  
 213 外部記憶部, 214 伸張部, 215 通信部, 216 インタ  
 フェース, 217 表示制御部, 218 入力制御部, 221 相互認証  
 モジュール, 222 課金処理モジュール, 223 記憶モジュール, 2  
 24 復号/暗号化モジュール, 225 データ検査モジュール, 231  
 復号ユニット, 232 乱数発生ユニット, 233 暗号化ユニット, 2  
 41 相互認証モジュール, 242 復号モジュール, 243 復号モジ  
 ュール, 244 伸張モジュール, 245 ウォータマーク付加モジュール

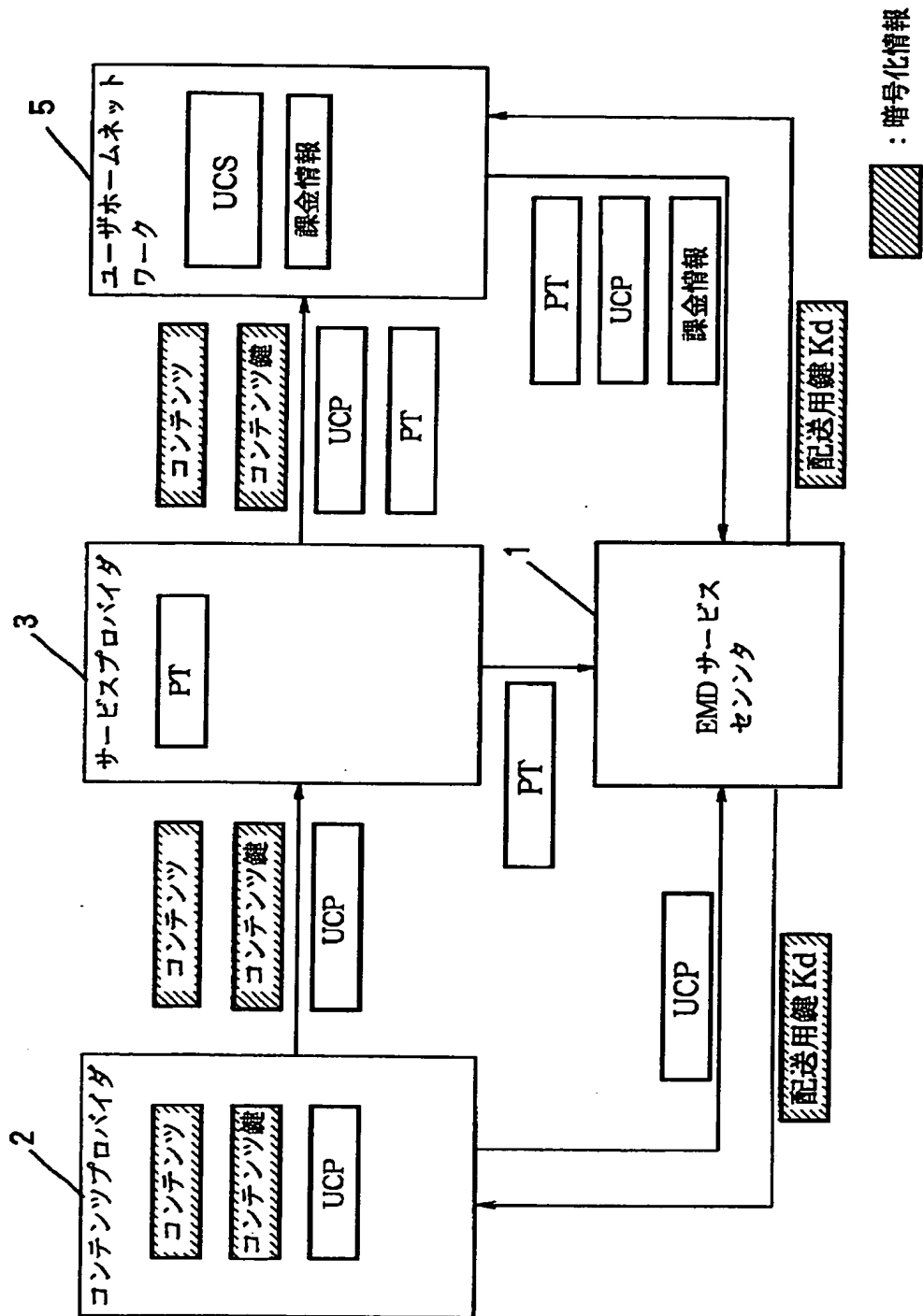
【書類名】

図面

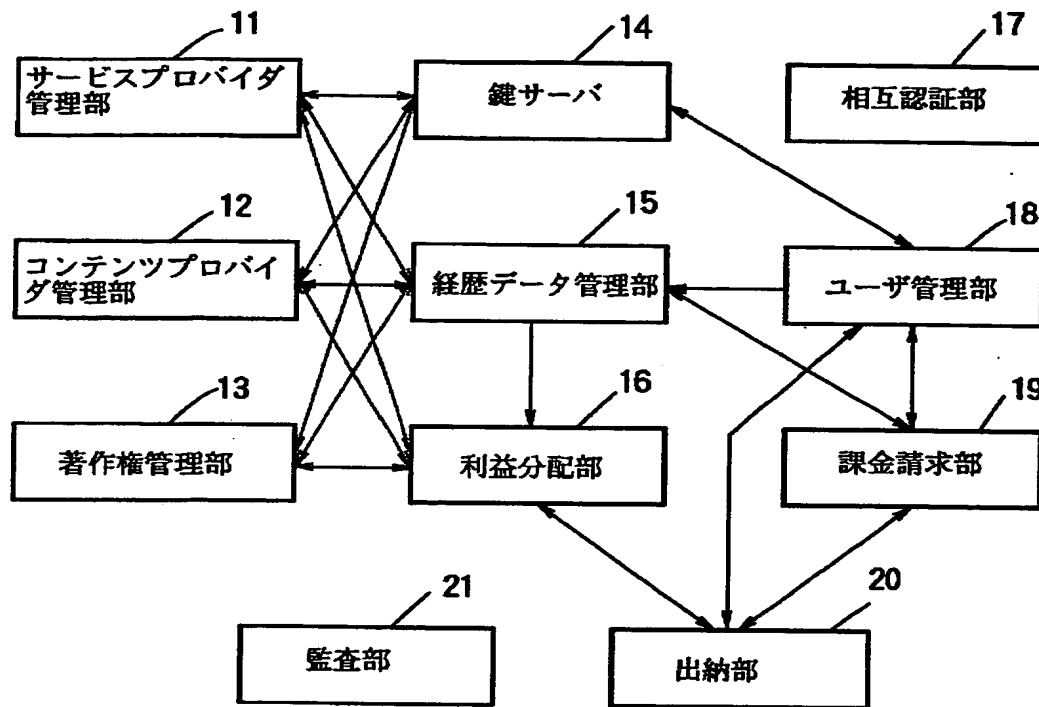
【図 1】



【図 2】

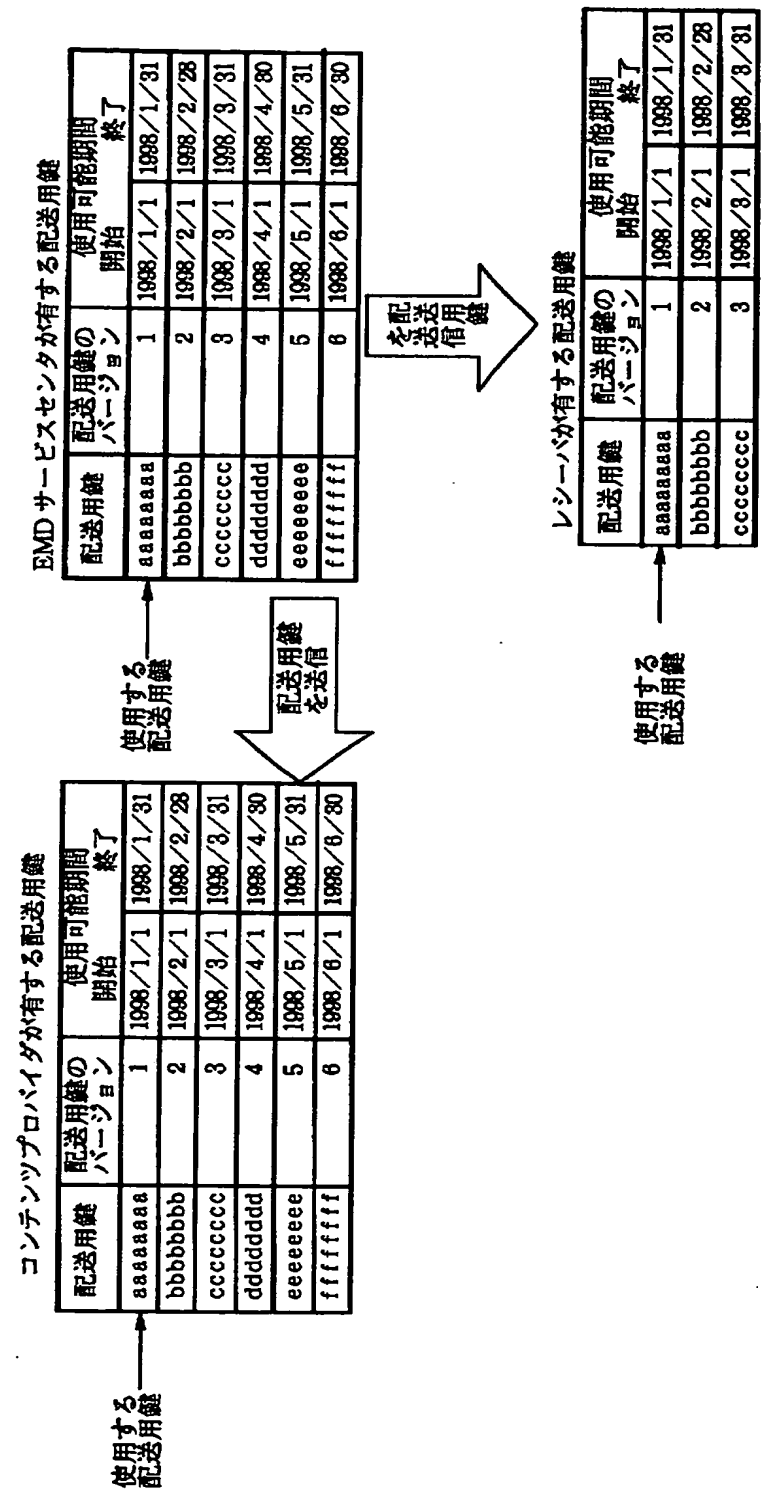


【図 3】

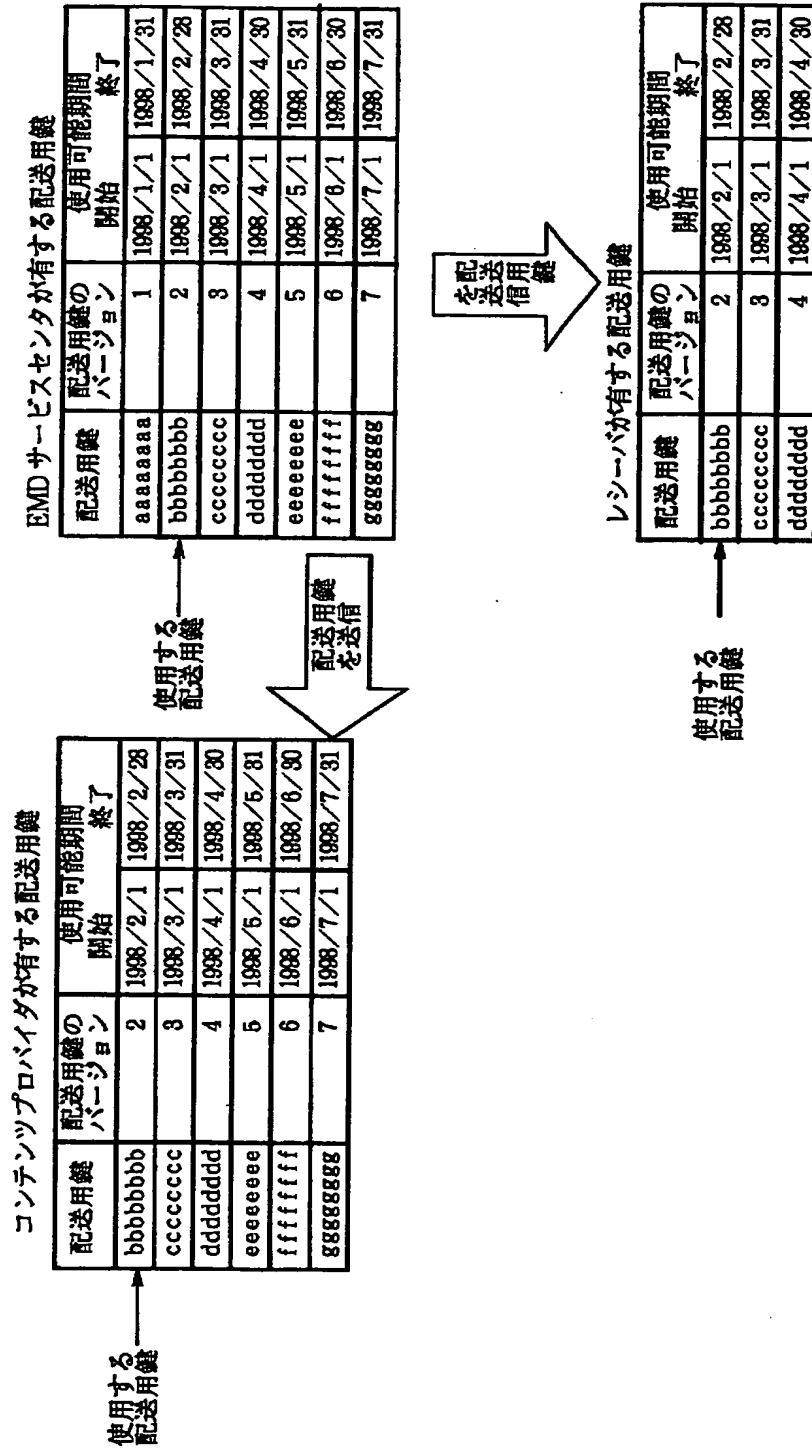


EMD サービスセンタ 1

【図 4】

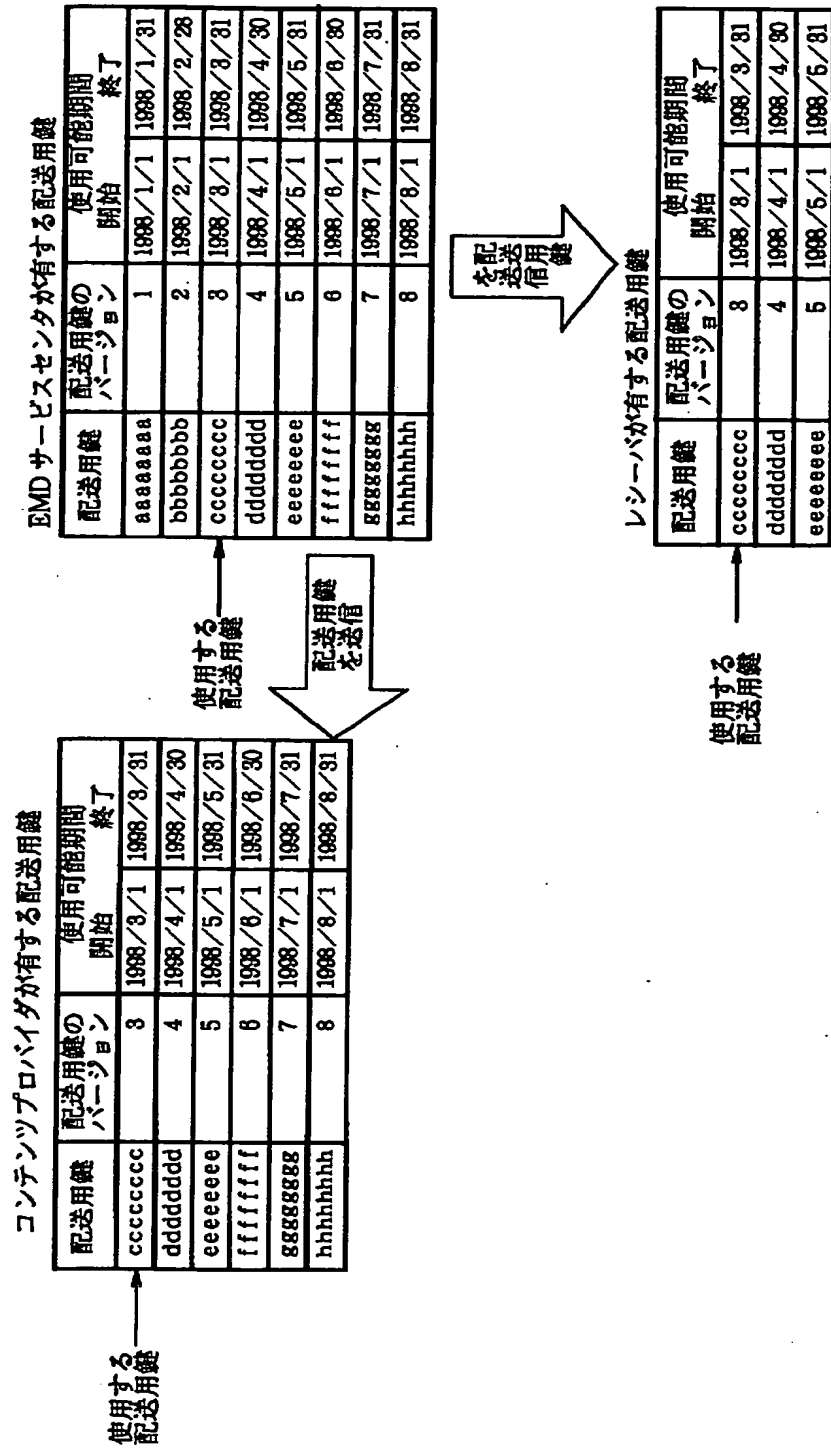


【図 5】

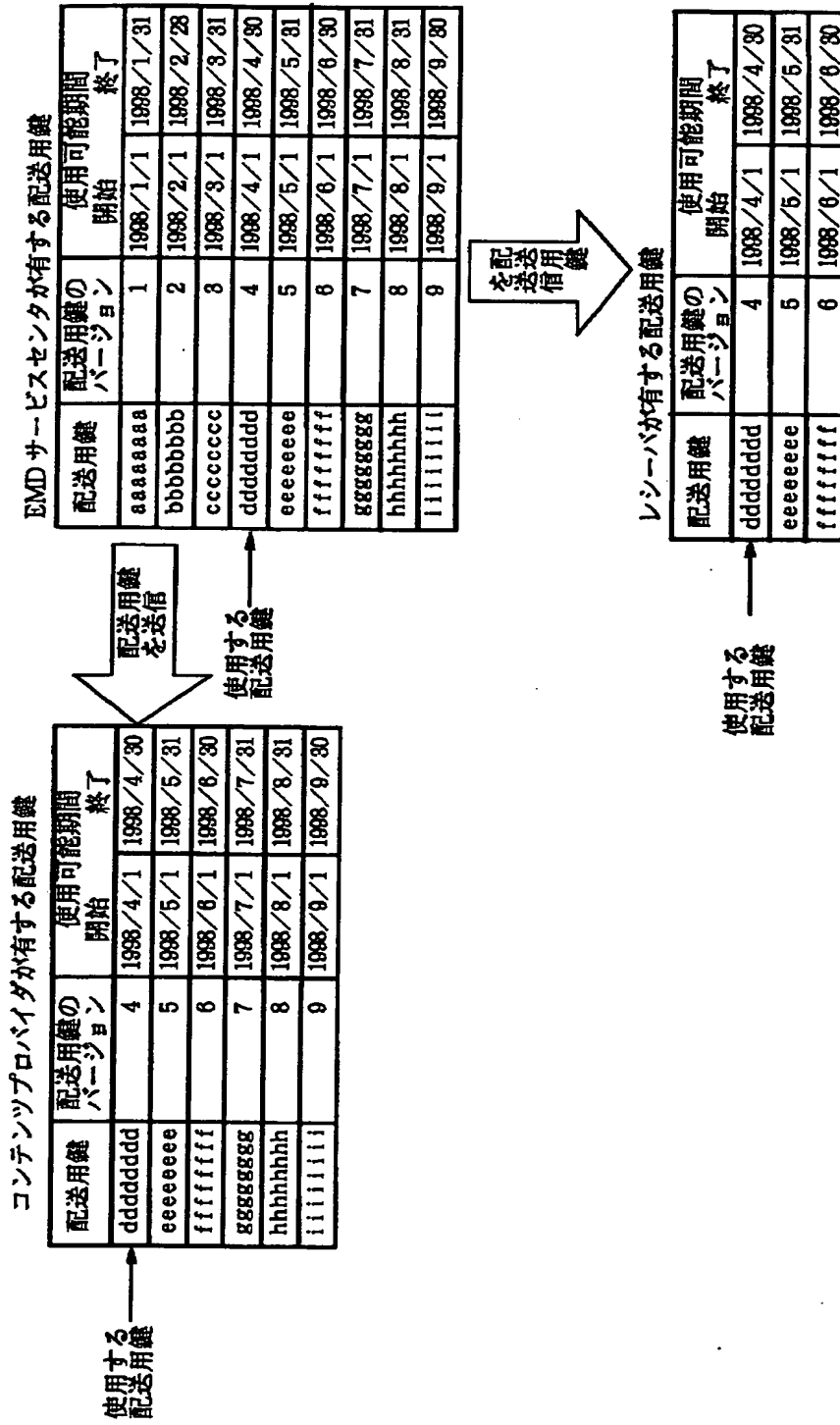




【図 6】



【図 7】

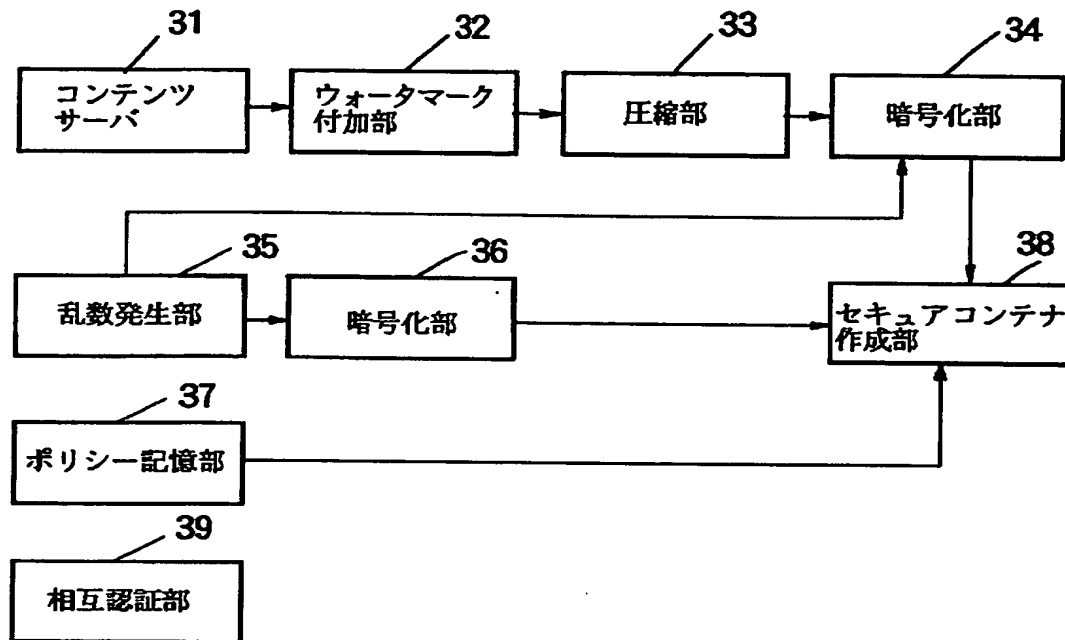


【図 8】

SAM の ID		SAM62 の ID	SAM212 の ID	SAM311 の ID
機器番号		レシーバ 51 の 機器番号(100 番)	レシーバ 201 の 機器番号(100 番)	レシーバ 301 の 機器番号(25 番)
決済 ID		ユーザ F の決済 ID	ユーザ F の決済 ID	ユーザ F の決済 ID
決済ユーザ情報	氏名	ユーザ F の氏名	ユーザ F の氏名	ユーザ F の氏名
	住所	ユーザ F の住所	ユーザ F の住所	ユーザ F の住所
	電話番号	ユーザ F の電話番号	ユーザ F の電話番号	ユーザ F の電話番号
	決済機関情報	ユーザ F の決済情報	ユーザ F の決済情報	ユーザ F の決済情報
	生年月日	ユーザ F の生年月日	ユーザ F の生年月日	ユーザ F の生年月日
	年齢	ユーザ F の年齢	ユーザ F の年齢	ユーザ F の年齢
	性別	ユーザ F の性別	ユーザ F の性別	ユーザ F の性別
	ユーザの ID	ユーザ F の ID	ユーザ F の ID	ユーザ F の ID
	パスワード	ユーザ F のパスワード	ユーザ F のパスワード	ユーザ F のパスワード
従属ユーザ情報	氏名		ユーザ A の氏名	ユーザ A の氏名
	住所		ユーザ A の住所	ユーザ A の住所
	電話番号		ユーザ A の電話番号	ユーザ A の電話番号
	生年月日		ユーザ A の生年月日	ユーザ A の生年月日
	性別		ユーザ A の性別	ユーザ A の性別
	ユーザの ID		ユーザ A の ID	ユーザ A の ID
	パスワード		ユーザ A のパスワード	ユーザ A のパスワード
⋮				
利用ポイント情報		レシーバ 51 の利用 ポイント情報	レシーバ 201 の利用 ポイント情報	レシーバ 301 の利用 ポイント情報

## システム登録情報

【図 9】



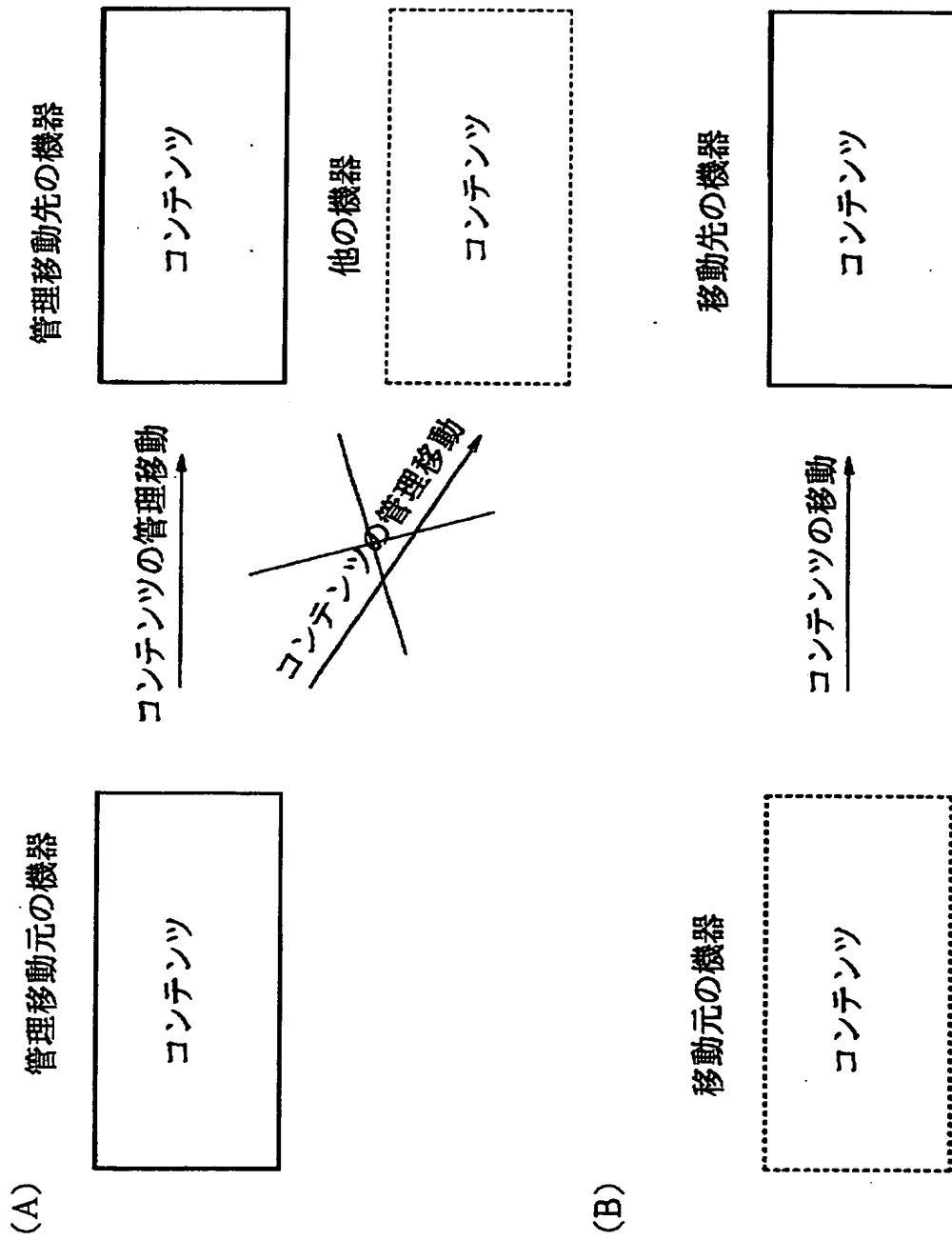
コンテンツプロバイダ 2

【図 10】

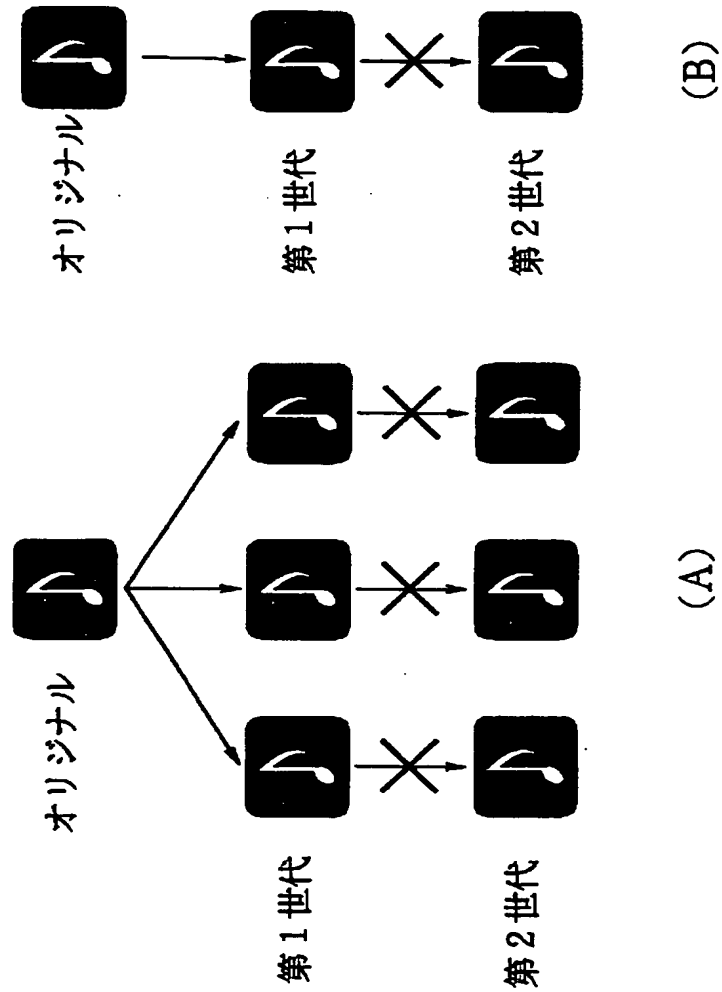
コンテンツの ID	コンテンツ A の ID	
コンテンツプロバイダの ID	コンテンツプロバイダ 2 の ID	
UCP の ID	UCPA の ID	
UCP 有効期限	UCPA の有効期限	
利用条件 10	ユーザ条件 10	200 ポイント以上
	機器条件 10	条件なし
利用内容 11	ID 11	利用内容 11 の ID
	形式 11	買い取り再生
	パラメータ 11	××××
	管理移動許可情報	可
利用内容 12	ID 12	利用内容 12 の ID
	形式 12	第 1 世代複製
	パラメータ 12	××××
	管理移動許可情報	可
利用内容 13	ID 13	利用内容 13 の ID
	形式 13	期間制限再生
	パラメータ 13	××××
	管理移動許可情報	可
利用内容 14	ID 14	利用内容 14 の ID
	形式 14	Pay Per Copy N
	パラメータ 14	N 回
	管理移動許可情報	不可
利用内容 15	ID 15	利用内容 15 の ID
	形式 15	形式 13→形式 11
	パラメータ	×××
	管理移動許可情報	可
利用内容 16	ID 16	利用内容 16 の ID
	形式 16	形式 11→形式 11
	パラメータ	×××
	管理移動許可情報	可

UCPA

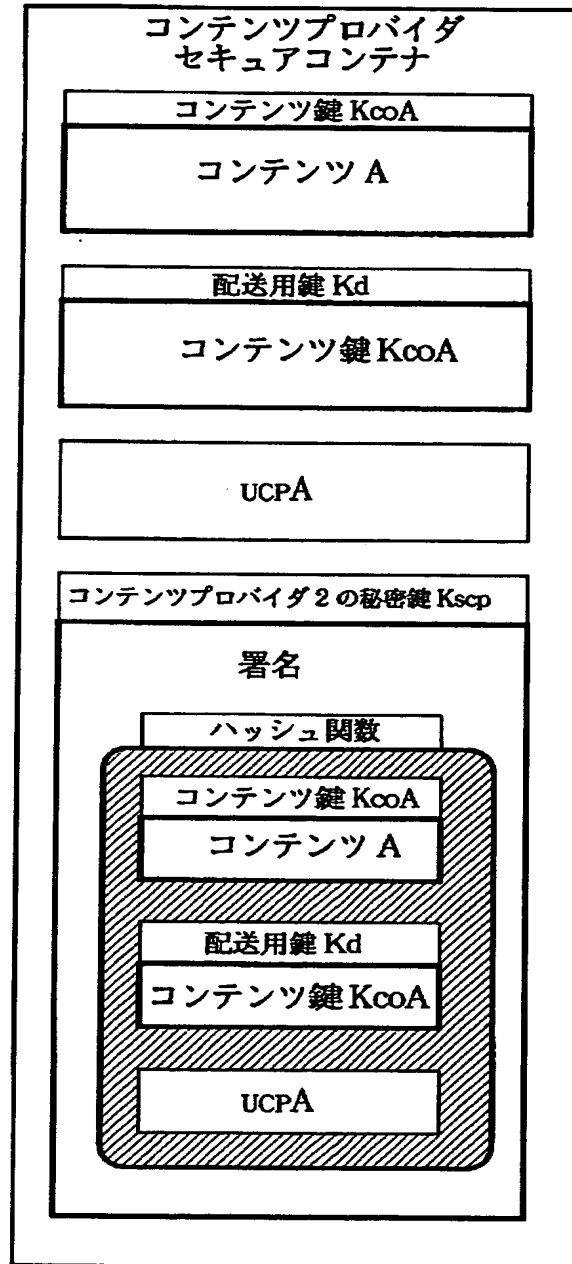
【図 1 1】



【図 12】

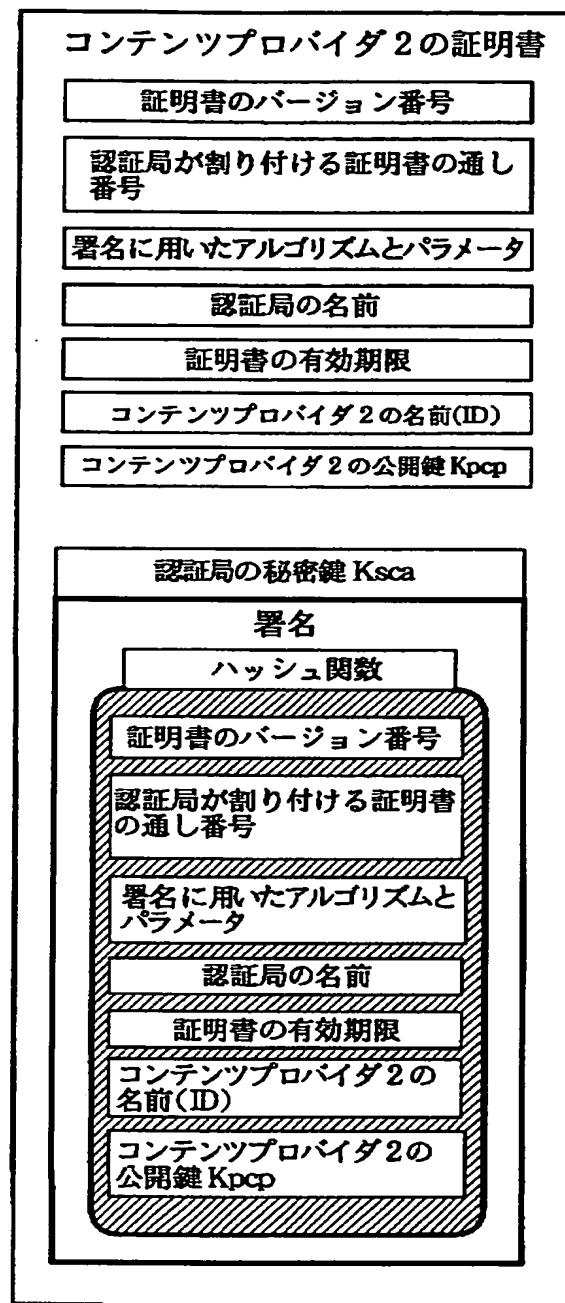


【図 13】

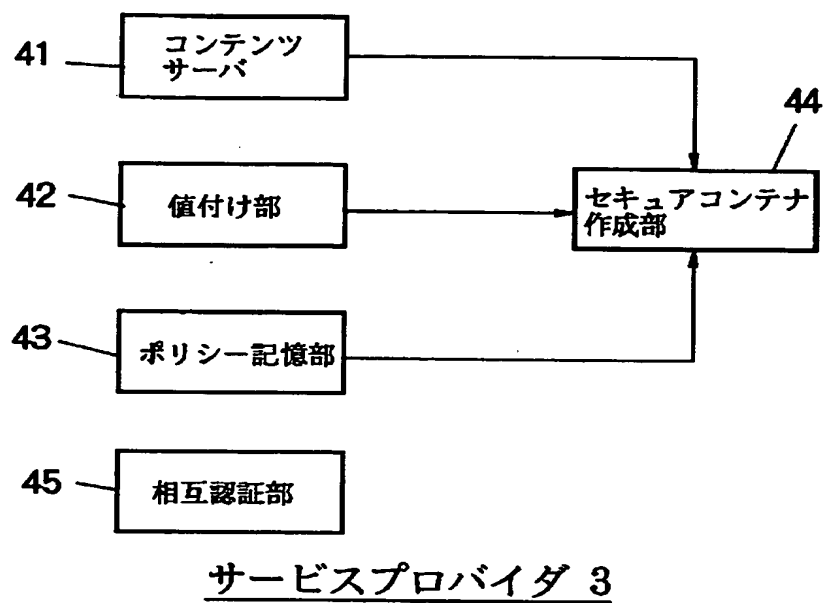




【図 14】



【図 1 5】



【図 16】

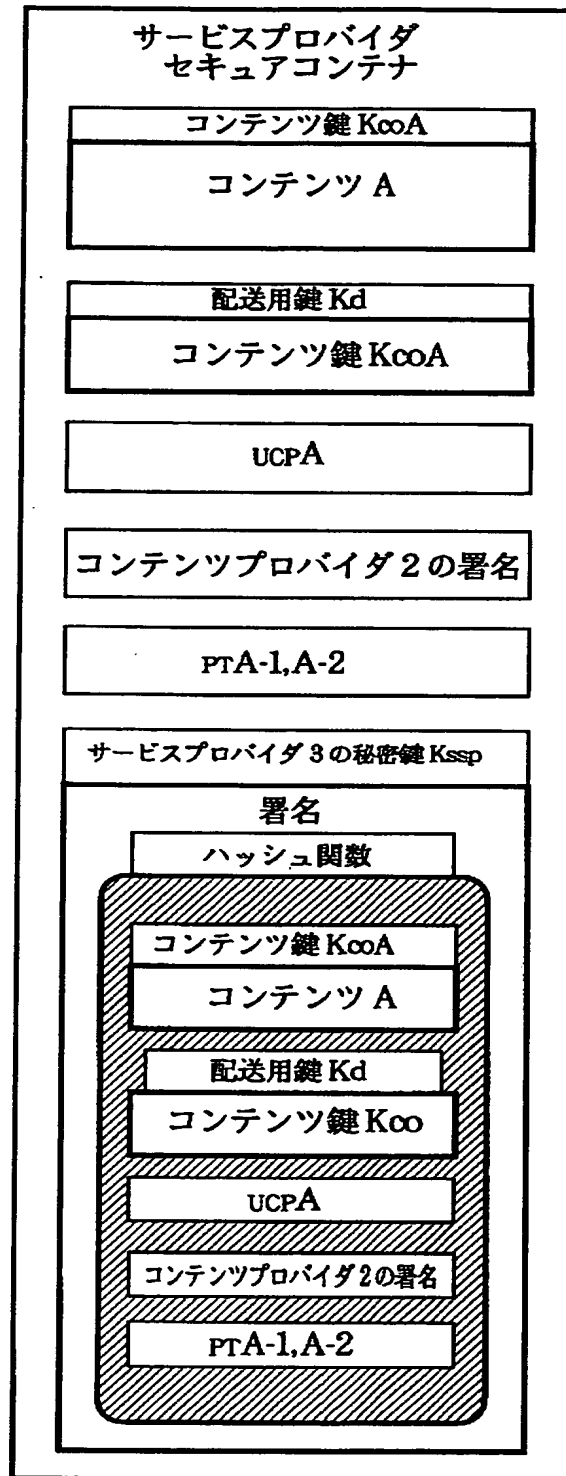
コンテンツの ID	コンテンツ A の ID	
コンテンツ プロバイダの ID	コンテンツプロバイダ 2 の ID	
UCP の ID	ucpA の ID	
サービス プロバイダの ID	サービスプロバイダ 3 の ID	
PT の ID	ptA-2 の ID	
PT の有効期限	ptA-2 の有効期限	
価格条件 20	ユーザ条件 20	女性
	機器条件 20	条件なし
価格内容 21	1,000 円	
価格内容 22	300 円	
価格内容 23	50 円	
価格内容 24	150 円	
価格内容 25	1980 円	
価格内容 26	500 円	

(B)

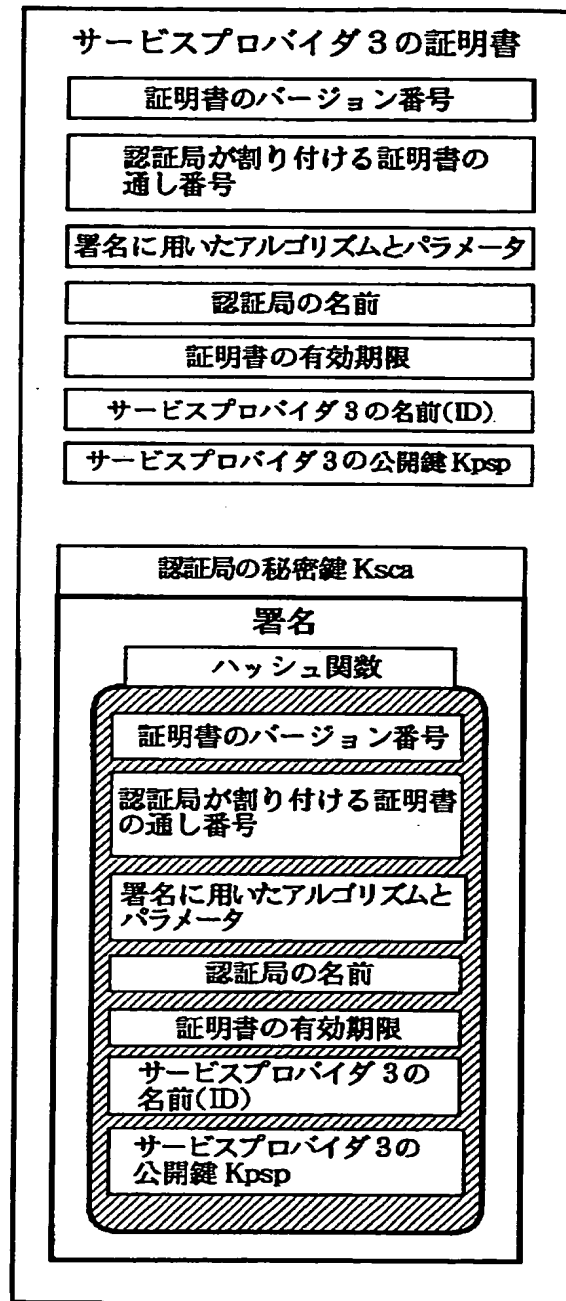
コンテンツの ID	コンテンツ A の ID		
コンテンツ プロバイダの ID	コンテンツプロバイダ 2 の ID		
UCP の ID	ucpA の ID		
サービス プロバイダの ID	サービスプロバイダ 3 の ID		
PT の ID	ptA-1 の ID		
PT の有効期限	ptA-1 の有効期限		
価格条件 10	ユーザ条件 10	男性	
	機器条件 10	条件なし	
価格内容 11	2,000 円		
価格内容 12	600 円		
価格内容 13	100 円		
価格内容 14	300 円		
価格内容 15	1950 円		
価格内容 16	1000 円		

(A)

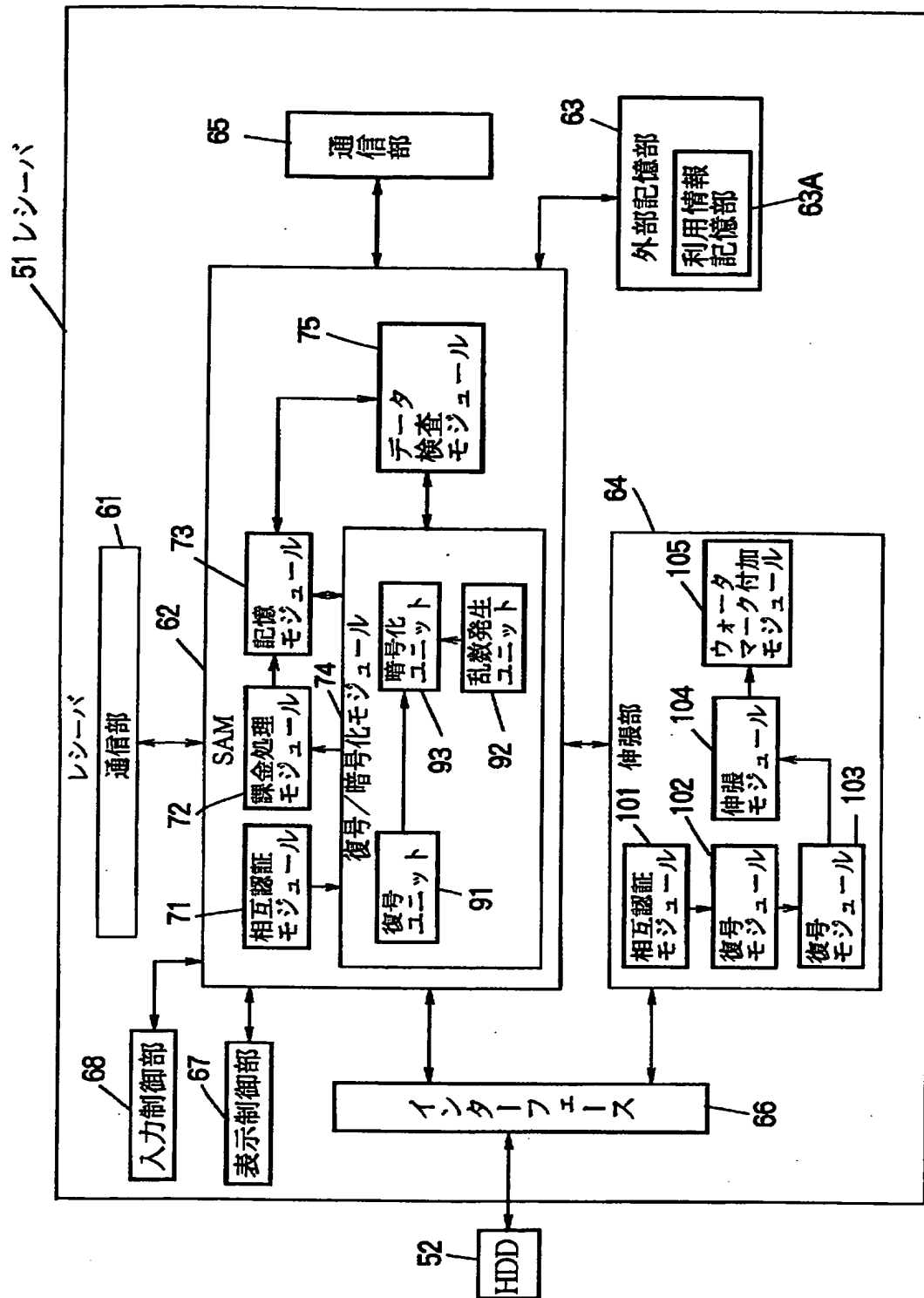
【図 17】



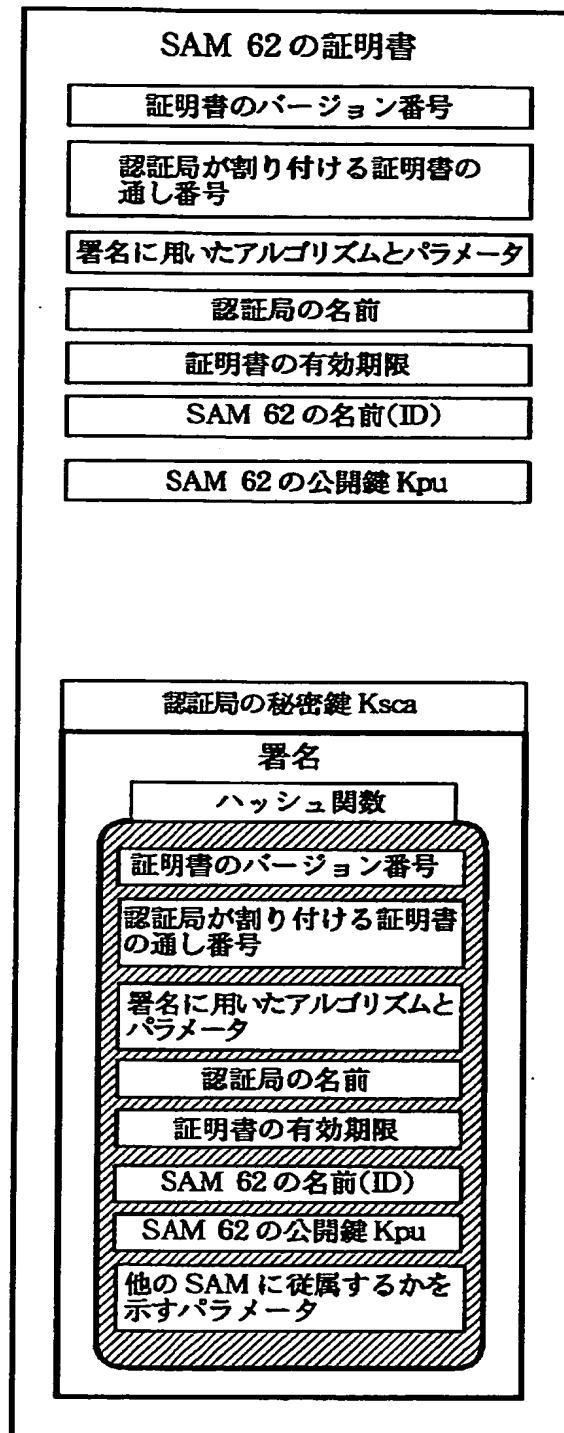
【図 18】



【図 19】



【図 20】



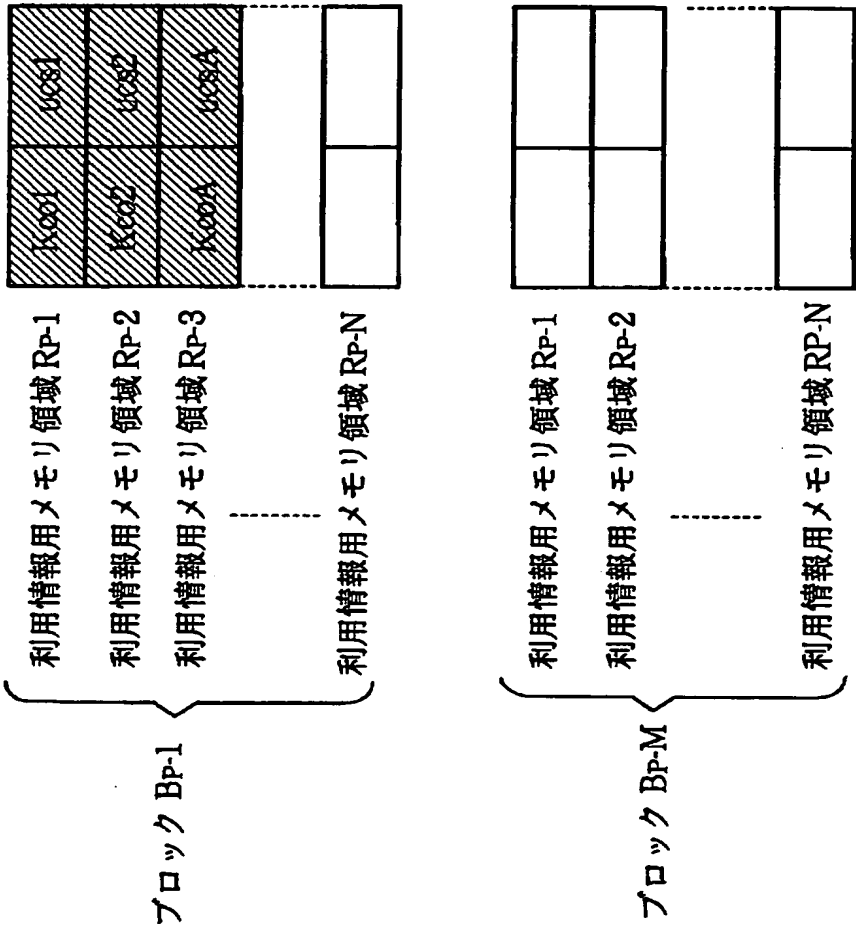
【図 2 1】

コンテンツの ID		コンテンツ A の ID
コンテンツ プロバイダの ID		コンテンツプロバイダ 2 の ID
UCP の ID		ucpA の ID
UCP の有効期限		ucpA の有効期限
サービス プロバイダの ID		サービスプロバイダ 3 の ID
PT の ID		ptA-1 の ID
PT の有効期限		ptA-1 の有効期限
UCS の ID		ucsA の ID
SAM の ID		SAM62 の ID
ユーザの ID		ユーザ F の ID
利用 内 容	ID	利用内容 13 の ID
	形式	期間制限再生
	パラメータ	× × ×
	管理移動 状態情報	管理移動元 : SAM62 の ID、 管理移動先 : SAM62 の ID
利用状態情報		× × ×

ucsA



【図 2 2】



利用情報記憶部 63A

【図 2 3】

コンテンツの ID		コンテンツ A の ID
コンテンツ プロバイダの ID		コンテンツプロバイダ 2 の ID
UCP の ID		ucpA の ID
UCP の有効期限		ucpA の有効期限
サービス プロバイダの ID		サービスプロバイダ 3 の ID
PT の ID		PTA-1 の ID
PT の有効期限		PTA-1 の有効期限
UCS の ID		ucsA の ID
SAM の ID		SAM62 の ID
ユーザの ID		ユーザ F の ID
利用内容	ID	利用内容 13 の ID
	形式	期間制限再生
	パラメータ	× × ×
	管理移動 状態情報	管理移動元 : SAM62 の ID、 管理移動先 : SAM62 の ID

## 課金情報 A

【图 24】

SAM62 の公開鍵 Kpu	
SAM62 の秘密鍵 Ksu	
EMD サービスセンタ 1 の公開鍵 Kpesc	
認証局の公開鍵 Kpca	
保存用鍵 Ksave	
3 月分の配送用鍵 Kd	
<div style="border: 1px solid black; height: 100px; width: 100%; position: relative;"> <div style="position: absolute; top: 50%; left: 50%; transform: translate(-50%, -50%);">             ----- </div> </div>	
SAM62 の証明書	
基準情報 51	
課金情報	
<div style="border: 1px solid black; height: 100px; width: 100%; position: relative;"> <div style="position: absolute; top: 50%; left: 50%; transform: translate(-50%, -50%);">             ----- </div> </div>	
検査値 Hp-1	検査値 Hp-2 -----
-----	検査値 Hp-M

【図 25】

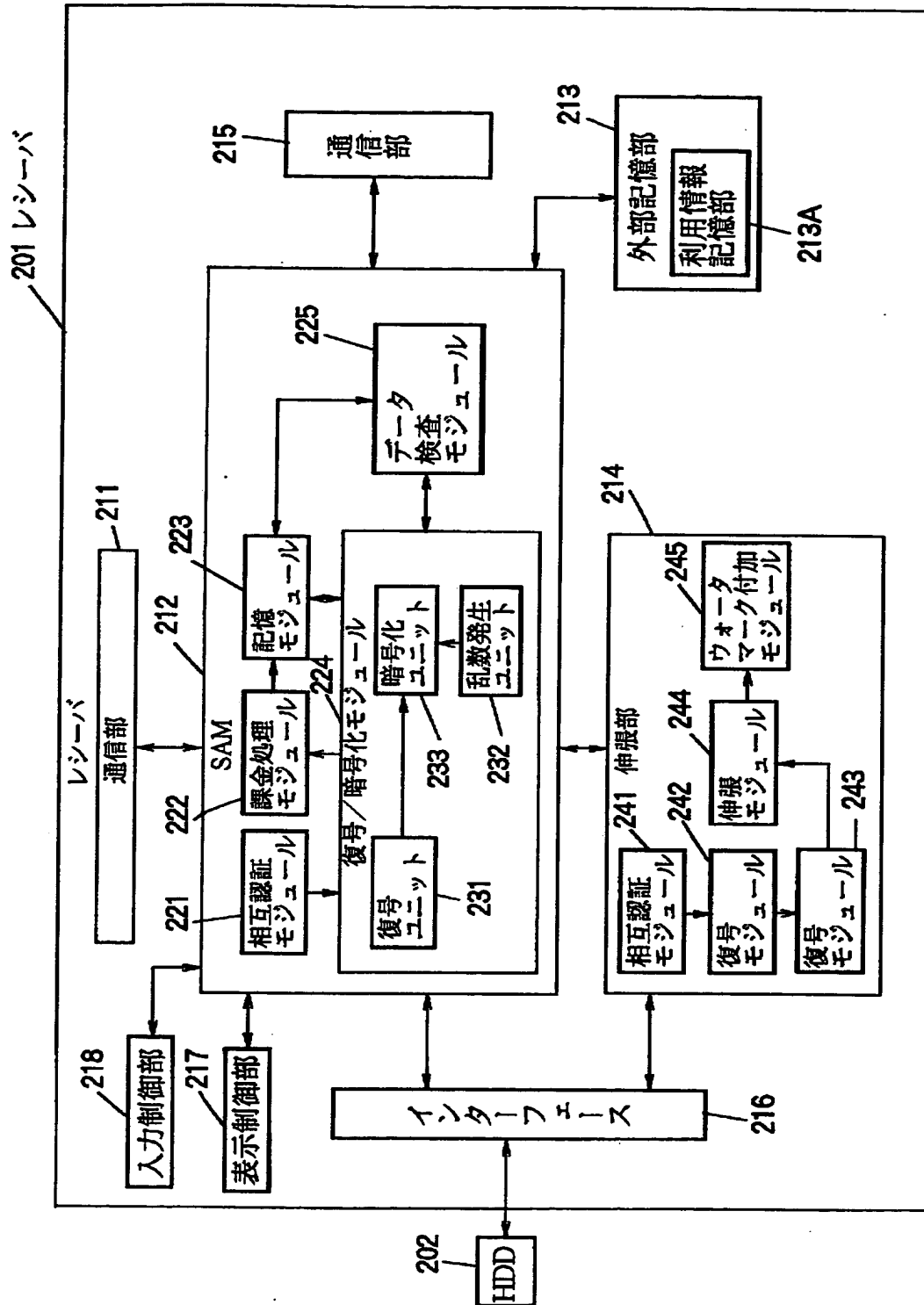
SAM の ID		SAM62 の ID
機器番号		レシーバ 51 の機器番号 (100 番)
決済 ID		ユーザ F の決済 ID
課金の上限額		正式登録時の課金の 上限額
決済 ユーザ 情報	氏名	ユーザ F の氏名
	住所	ユーザ F の住所
	電話番号	ユーザ F の電話番号
	決済機関情報	ユーザ F の決済機関情報
	生年月日	ユーザ F の生年月日
	年齢	ユーザ F の年齢
	性別	ユーザ F の性別
	ユーザの ID	ユーザ F の ID
	パスワード	ユーザ F のパスワード
従属 ユーザ 情報	氏名	
	住所	
	電話番号	
	生年月日	
	性別	
	ユーザの ID	
	パスワード	
利用ポイント情報		レシーバ 51 の利用 ポイント情報

基準情報 51

【図 26】

リスト部							対象 SAM 情報部		
SAM ID	ユーザ ID	購入処理	課金処理	課金機器	コンテンツ供給機器	状態フラグ	登録条件署名	登録リスト署名	
レシーバ 51の登録 条件 SAM62の ID	ユーザF のID	可	可	SAM62 のID	なし	制限 なし	××××	××××	
レシーバ 201の登録 条件 SAM212の ID	ユーザF のID	可	可	SAM212 のID	SAM62 のID	制限 なし	××××		
レシーバ 301の登録 条件 SAM312の ID	ユーザF のID	不可	不可	なし	SAM62 のID	制限 なし	××××		
							SAM62のID		
							××××		
							××××		
							3		
							対象 SAM ID		
							有効期限		
							バージョン番号		
							接続されている機器数		

【図 27】



【図 28】

SAM の ID		SAM212 の ID
機器番号		レシーバ 201 の機器番号 (100 番)
決済 ID		ユーザ F の決済 ID
課金の上限額		正式登録時の上限額
決済 ユーザ 情報	氏名	ユーザ F の氏名
	住所	ユーザ F の住所
	電話番号	ユーザ F の電話番号
	決済機関情報	ユーザ F の決済情報
	生年月日	ユーザ F の生年月日
	年齢	ユーザ F の年齢
	性別	ユーザ F の性別
	ユーザの ID	ユーザ F の ID
	パスワード	ユーザ F のパスワード
従属 ユーザ 情報	氏名	ユーザ A の氏名
	住所	ユーザ A の住所
	電話番号	ユーザ A の電話番号
	生年月日	ユーザ A の生年月日
	性別	ユーザ A の性別
	ユーザの ID	ユーザ A の ID
	パスワード	ユーザ A のパスワード
利用ポイント情報		レシーバ 201 の利用 ポイント情報

## 基準情報 201

【図 2 9】

リスト部									
SAM ID	ユーザ ID	購入処理	課金処理	課金機器	コンテンツ供給機器	状態フラグ	登録条件署名	登録リスト署名	
レシーバ 51 の登録 条件	SAM62 の ID	ユーザ F の ID	可	可	SAM62 の ID	なし	制限 なし	××××	××××
レシーバ 201 の登録 条件	SAM212 の ID	ユーザ F の ID	可	可	SAM212 の ID	SAM62 の ID	制限 なし	××××	××××

対象 SAM ID

SAM212 の ID

有効期限

××××

バージョン番号

××××

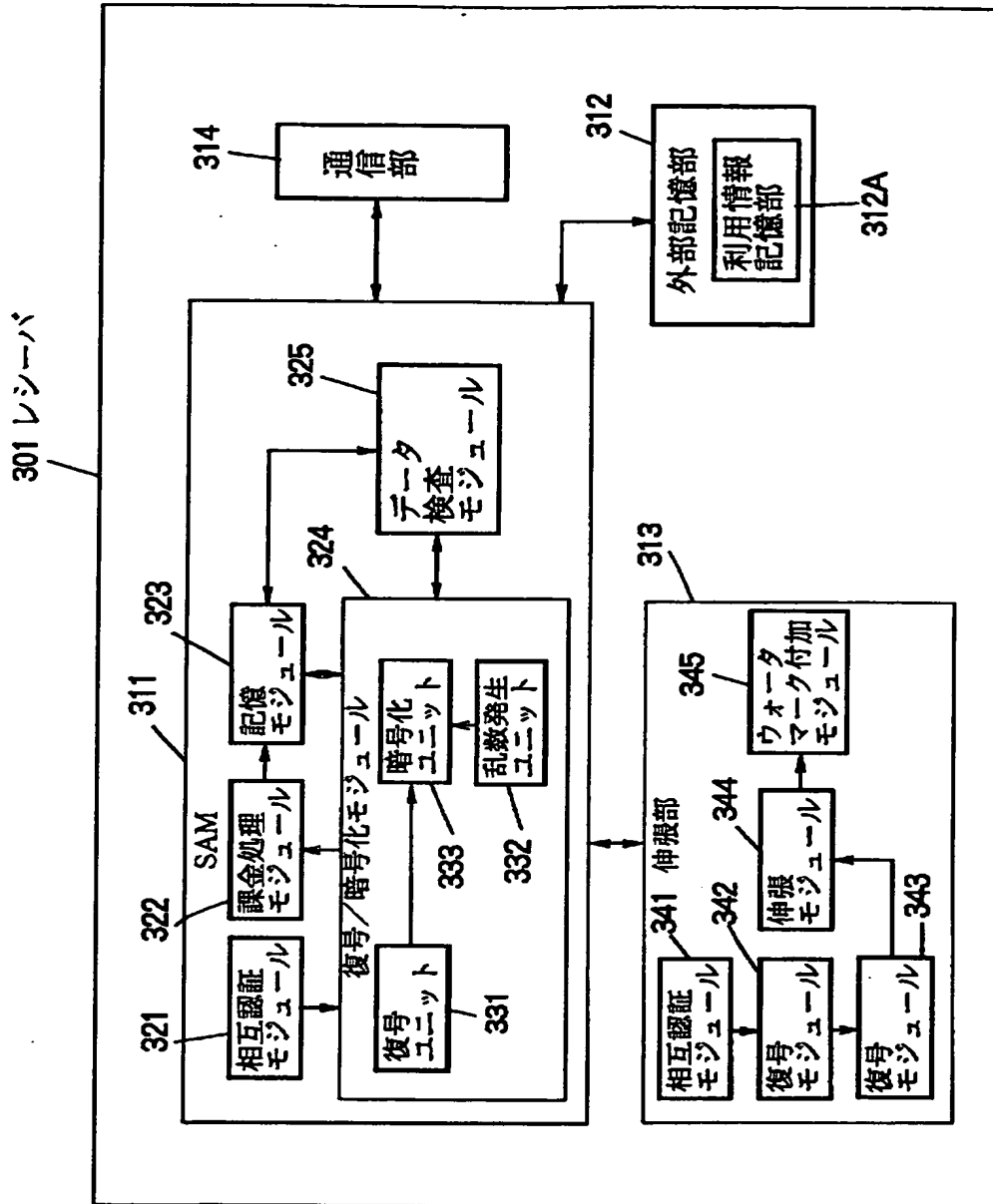
接続されている機器数

2

対象 SAM 情報部



【図 3 0】



【図 3 1】

SAM の ID		SAM311 の ID
機器番号		レシーバ 301 の機器番号 (25 番)
決済 ID		ユーザ F の決済 ID
課金の上限額		正式登録時の上限額
決済 ユーザ 情報	氏名	ユーザ F の氏名
	住所	ユーザ F の住所
	電話番号	ユーザ F の電話番号
	決済機関情報	ユーザ F の決済情報
	生年月日	ユーザ F の生年月日
	年齢	ユーザ F の年齢
	性別	ユーザ F の性別
	ユーザの ID	ユーザ F の ID
	パスワード	ユーザ F のパスワード
従属 ユーザ 情報	氏名	ユーザ A の氏名
	住所	ユーザ A の住所
	電話番号	ユーザ A の電話番号
	生年月日	ユーザ A の生年月日
	性別	ユーザ A の性別
	ユーザの ID	ユーザ A の ID
	パスワード	ユーザ A のパスワード
		⋮
利用ポイント情報		レシーバ 301 の ポイント情報

### 基準情報 301

【図 3 2】

レシーバ  
301の登録  
条件

SAM ID	ユーザ ID	購入 処理	課金 処理	課金機器	コンテンツ 供給機器	状態 フラグ
SAM311 の ID	ユーザ F の ID	不可	不可	なし	SAM62 の ID	制限 なし

リスト部

対象 SAM ID

SAM311 の ID

有効期限

××××

バージョン番号

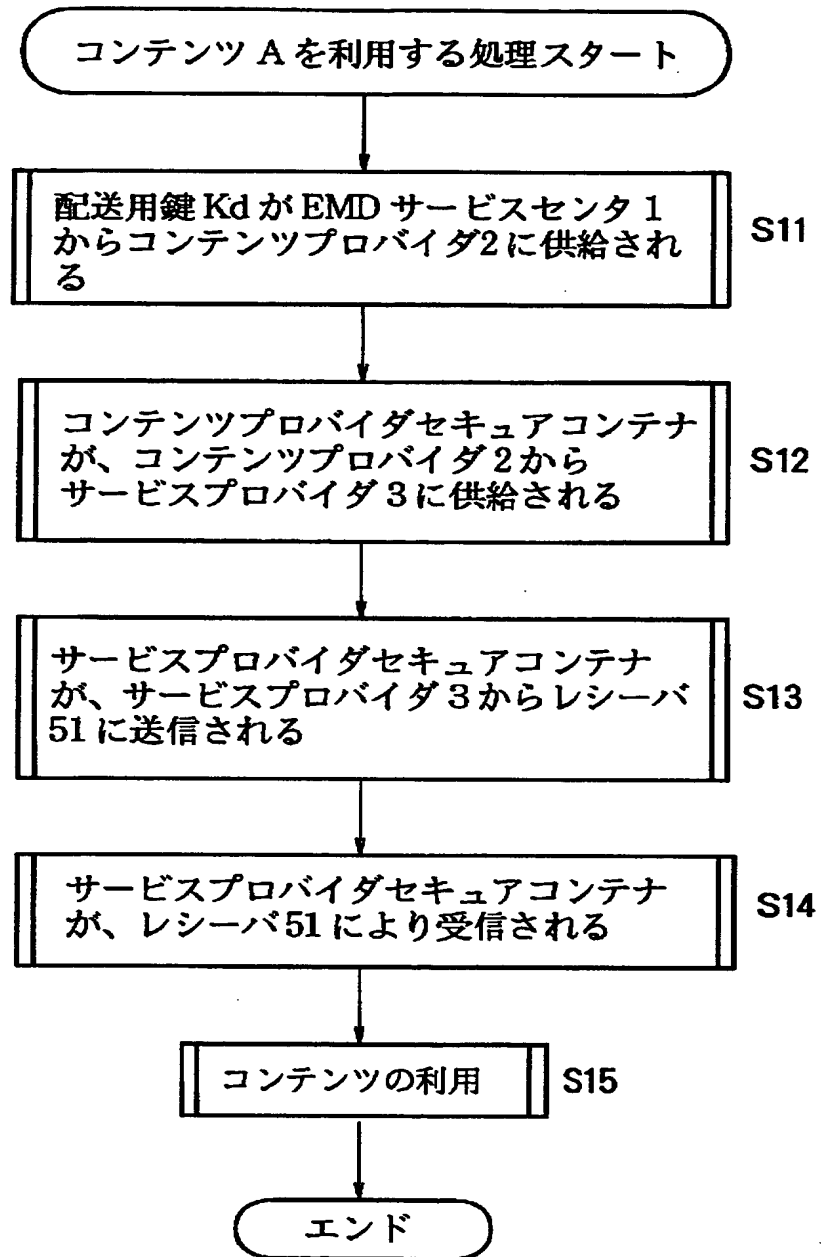
××××

接続されている機器数

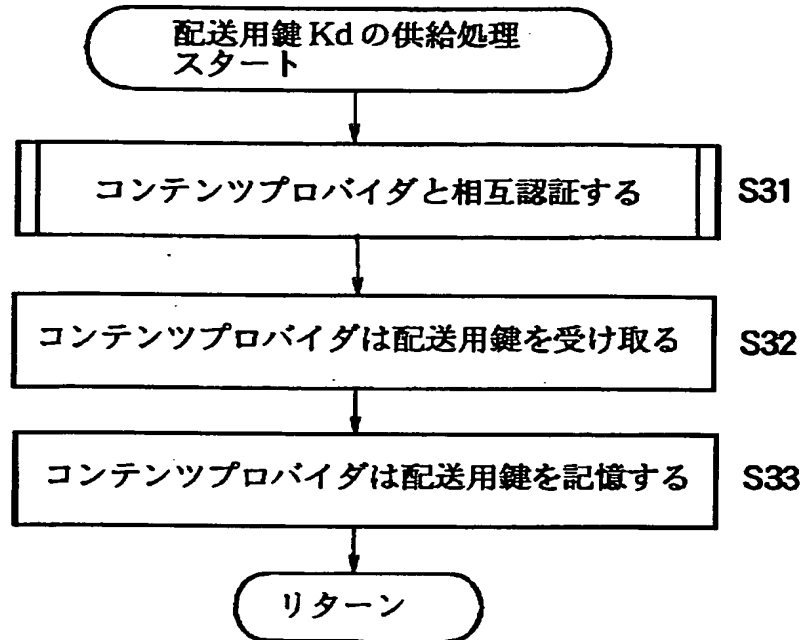
2

対象 SAM 情報部

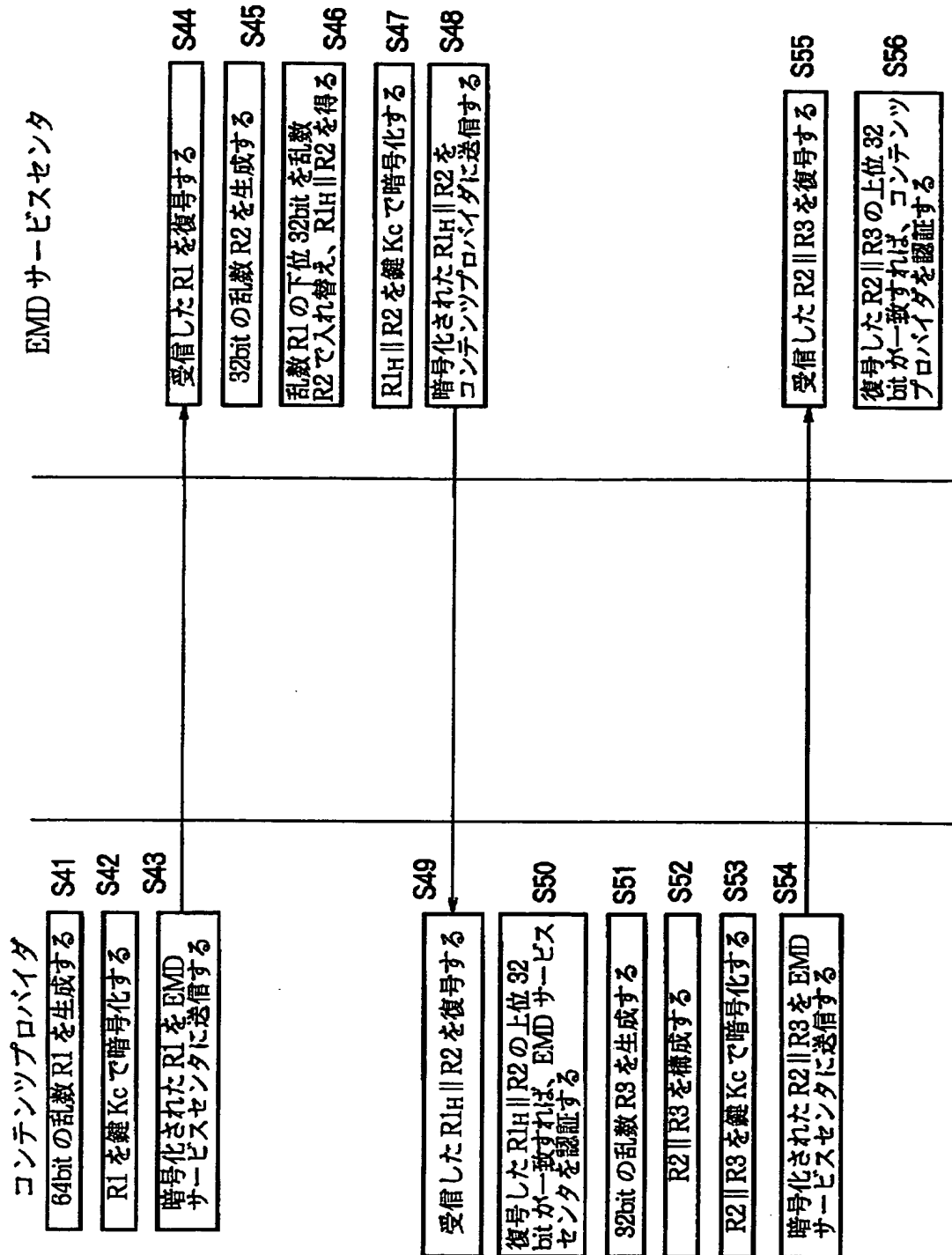
【図 33】



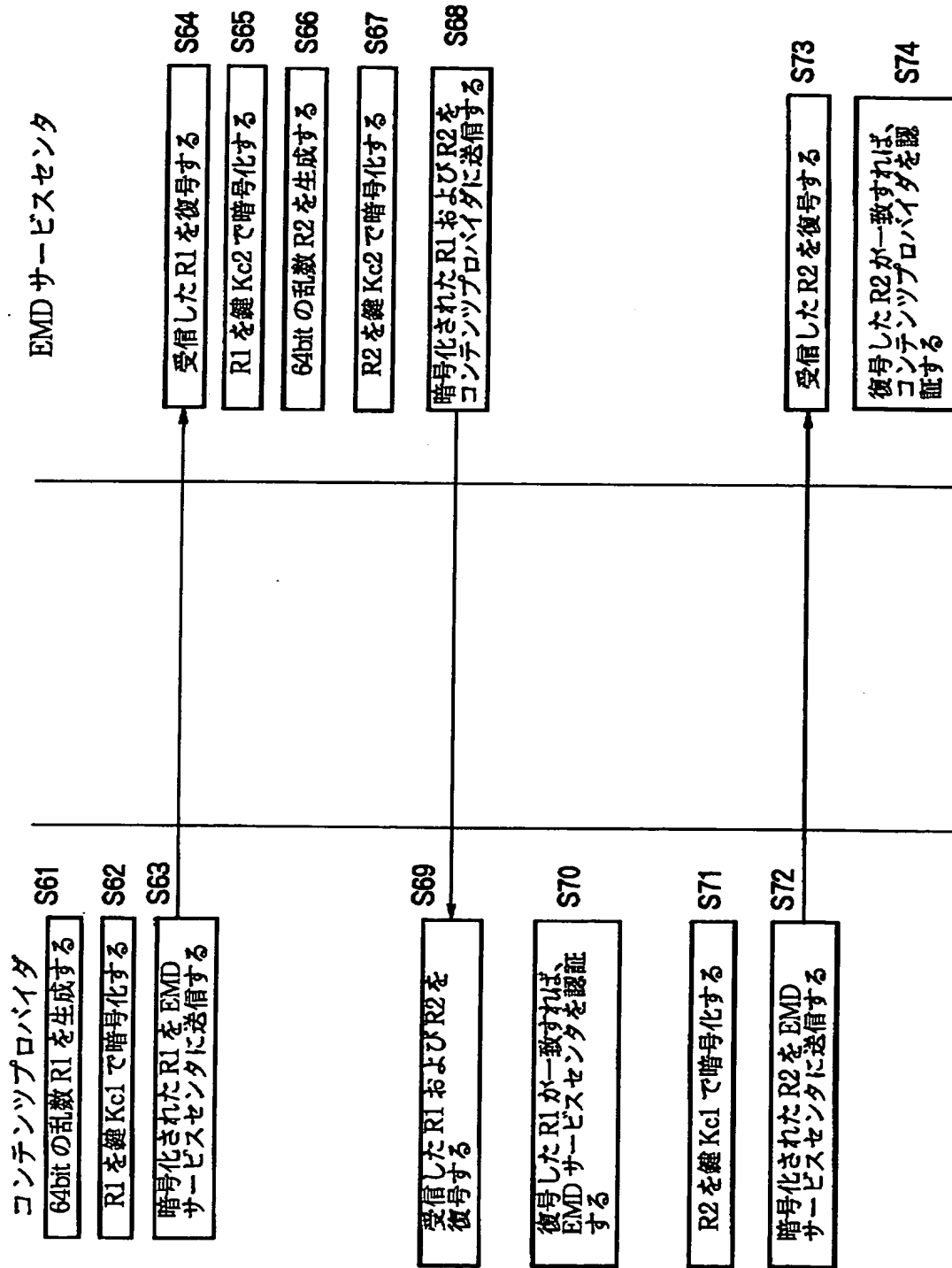
【図 34】



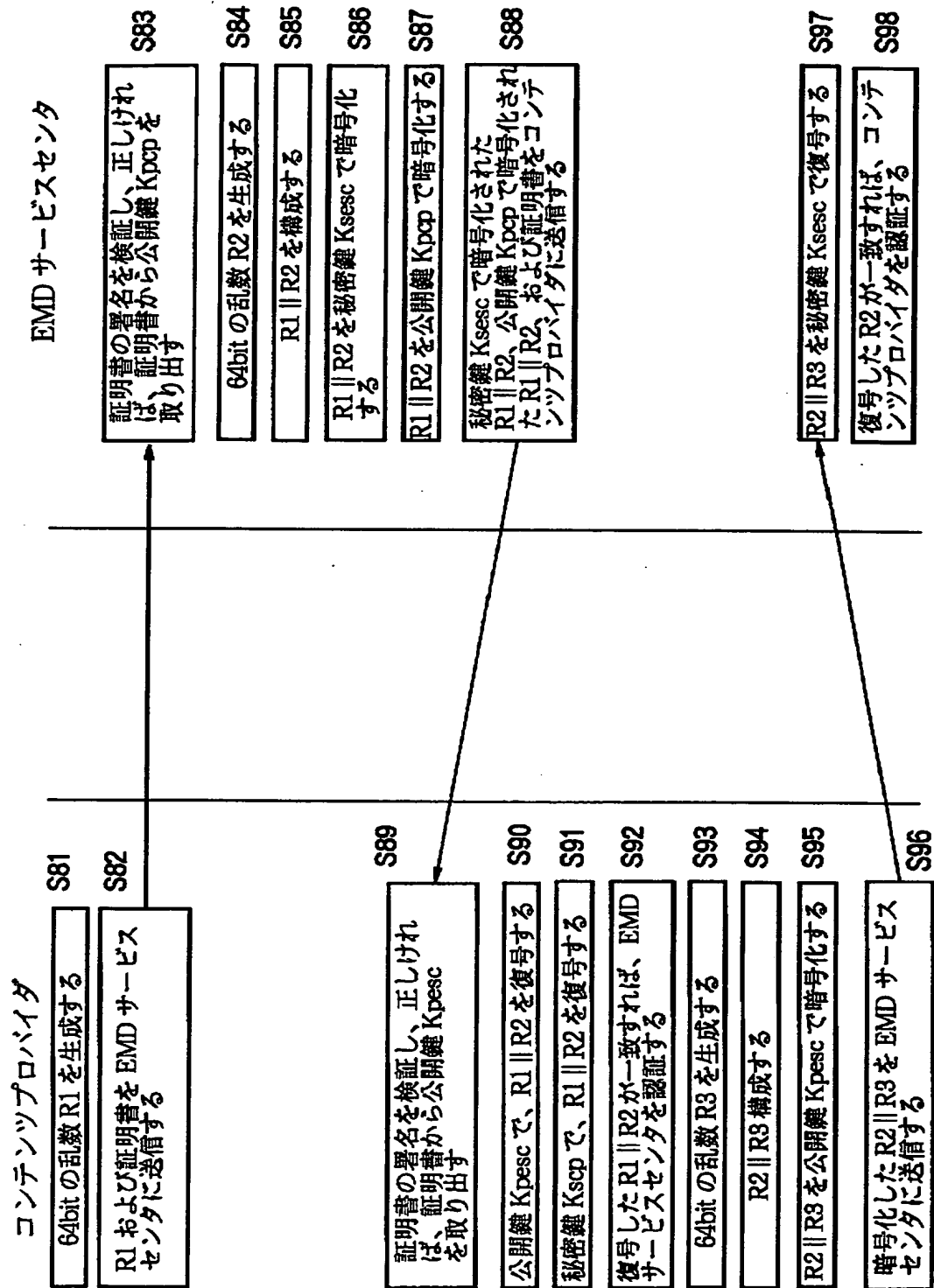
【図 3 5】



【図 3 6】

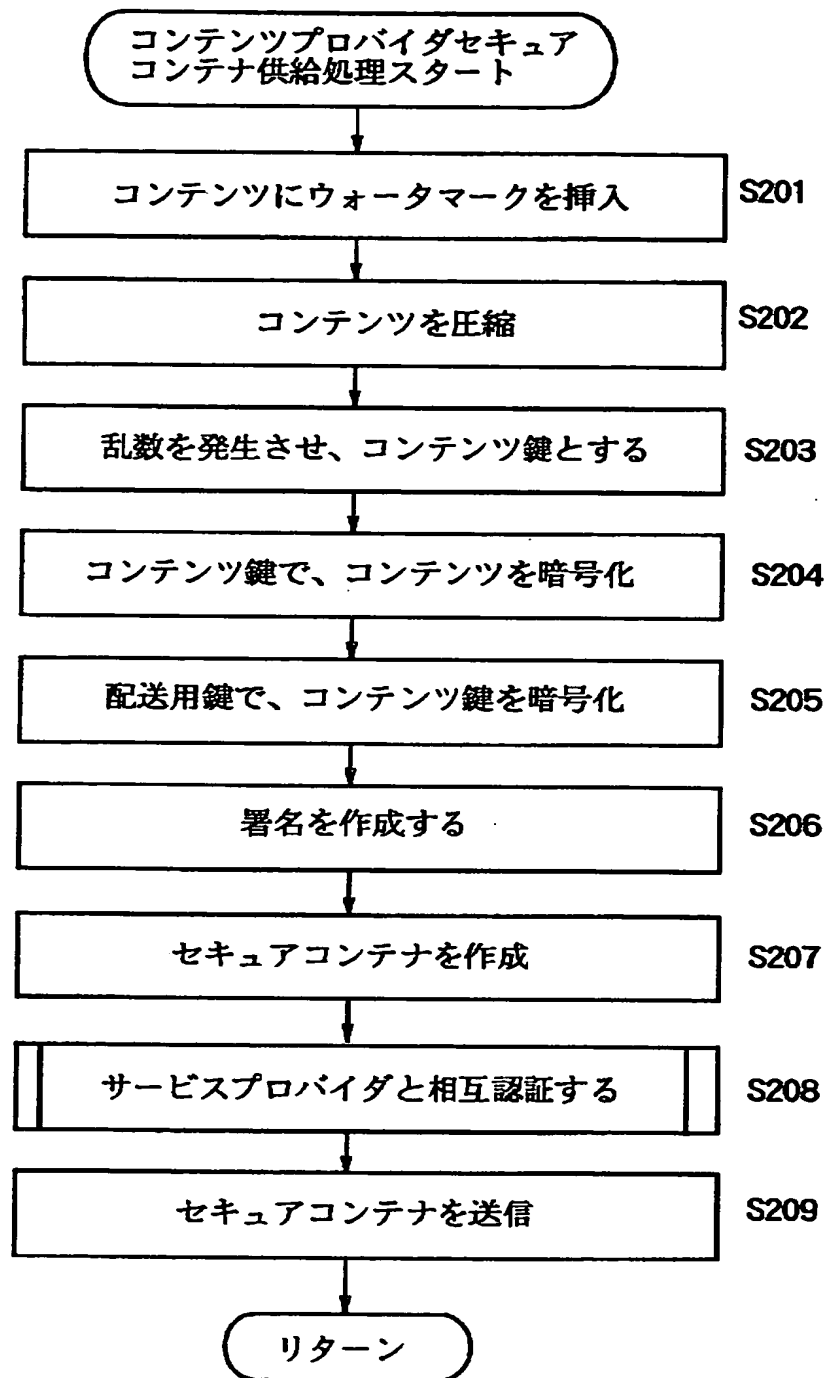


【図 37】

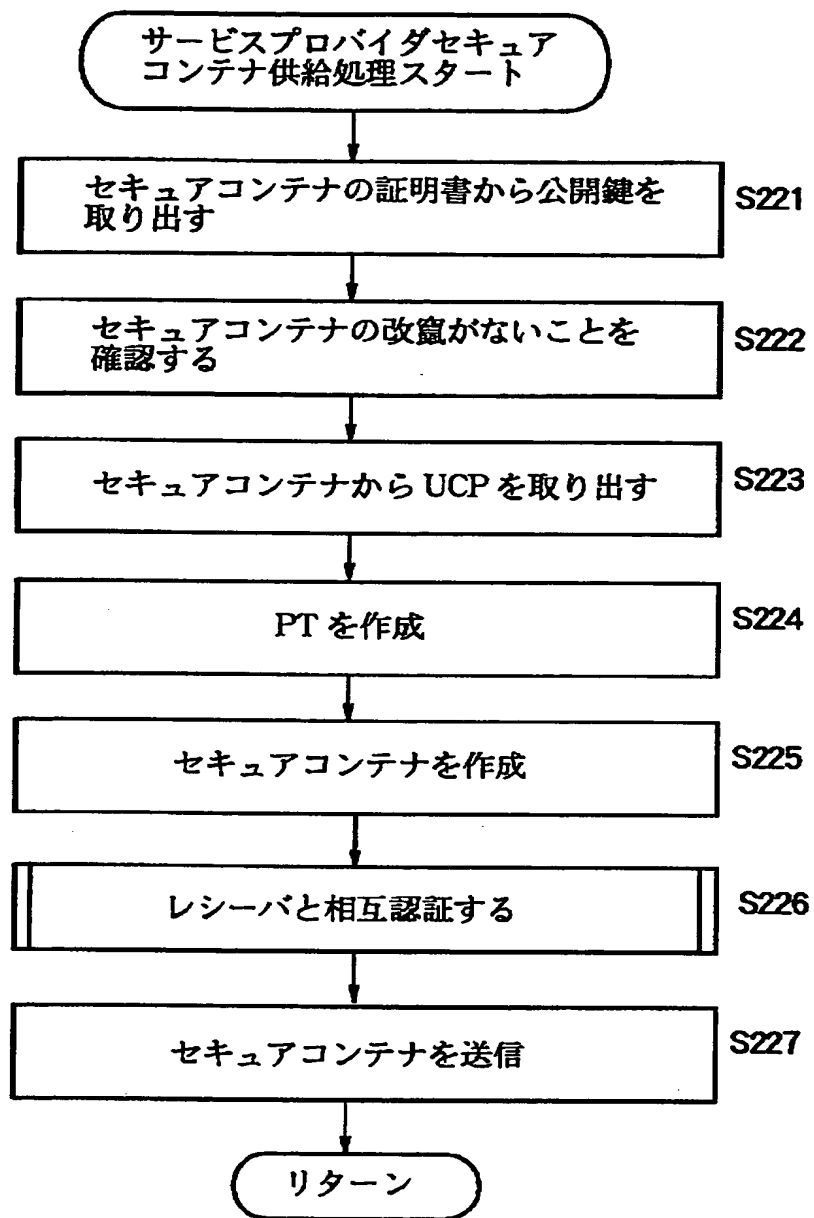




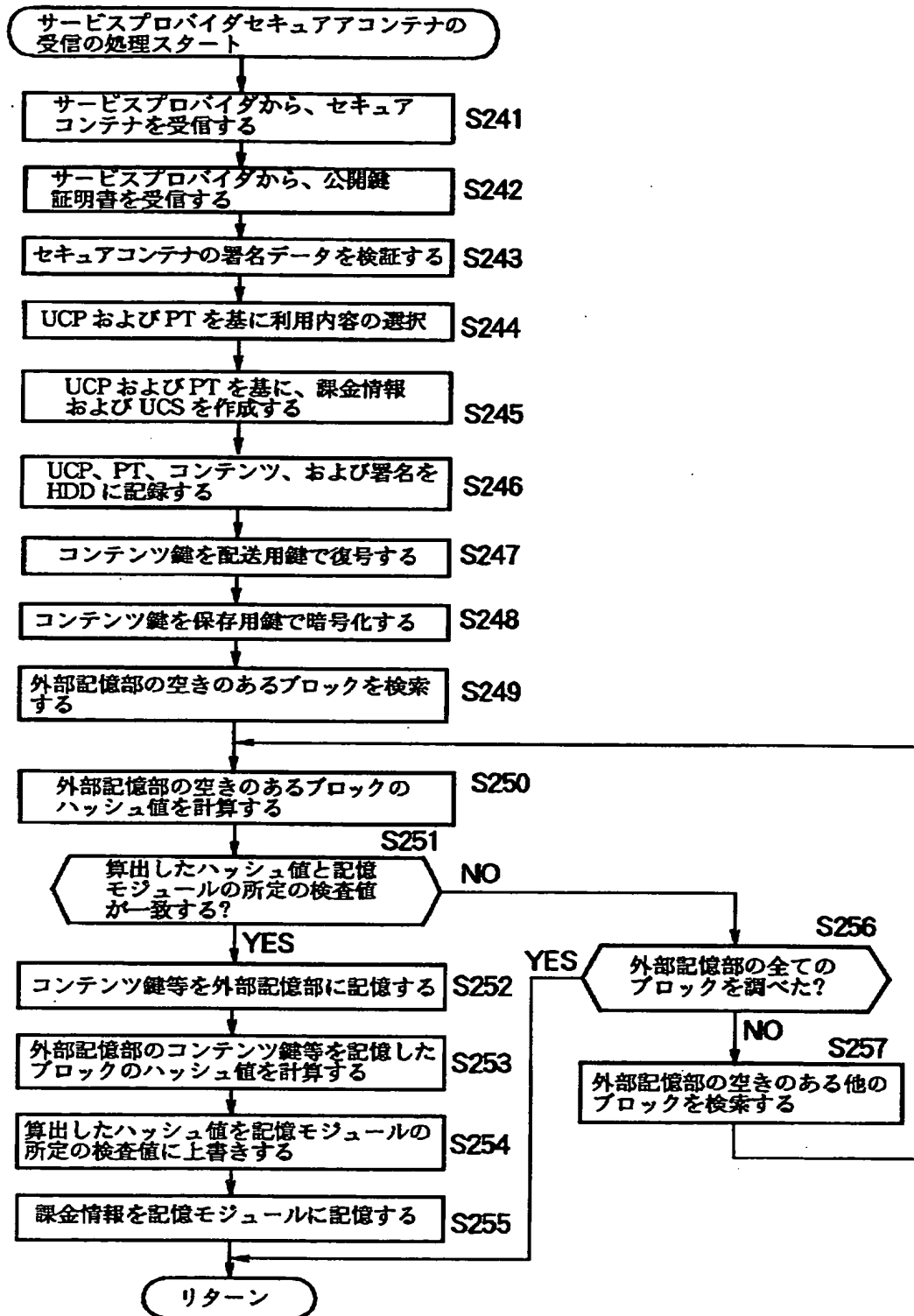
【図 38】



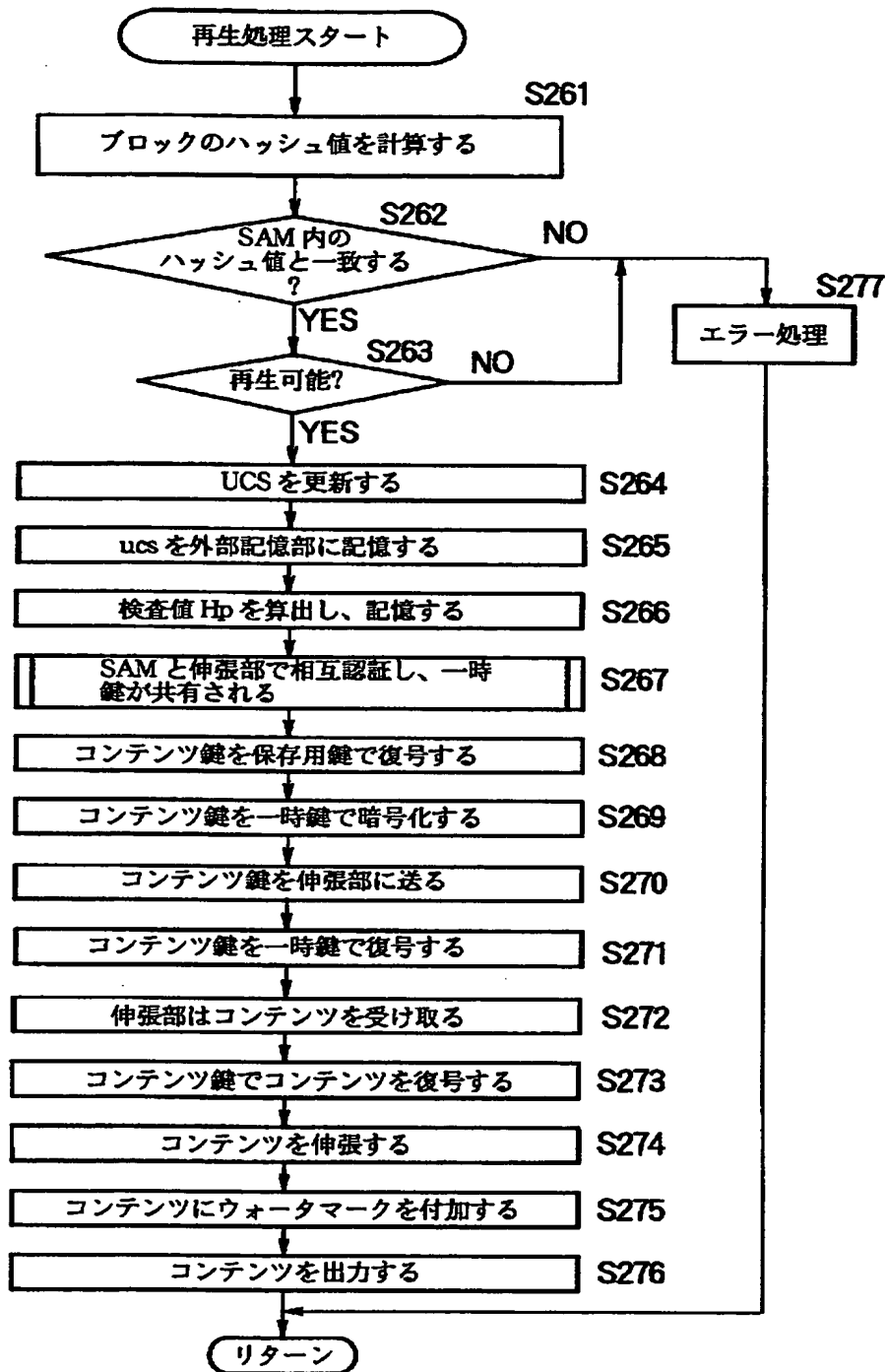
【図 39】



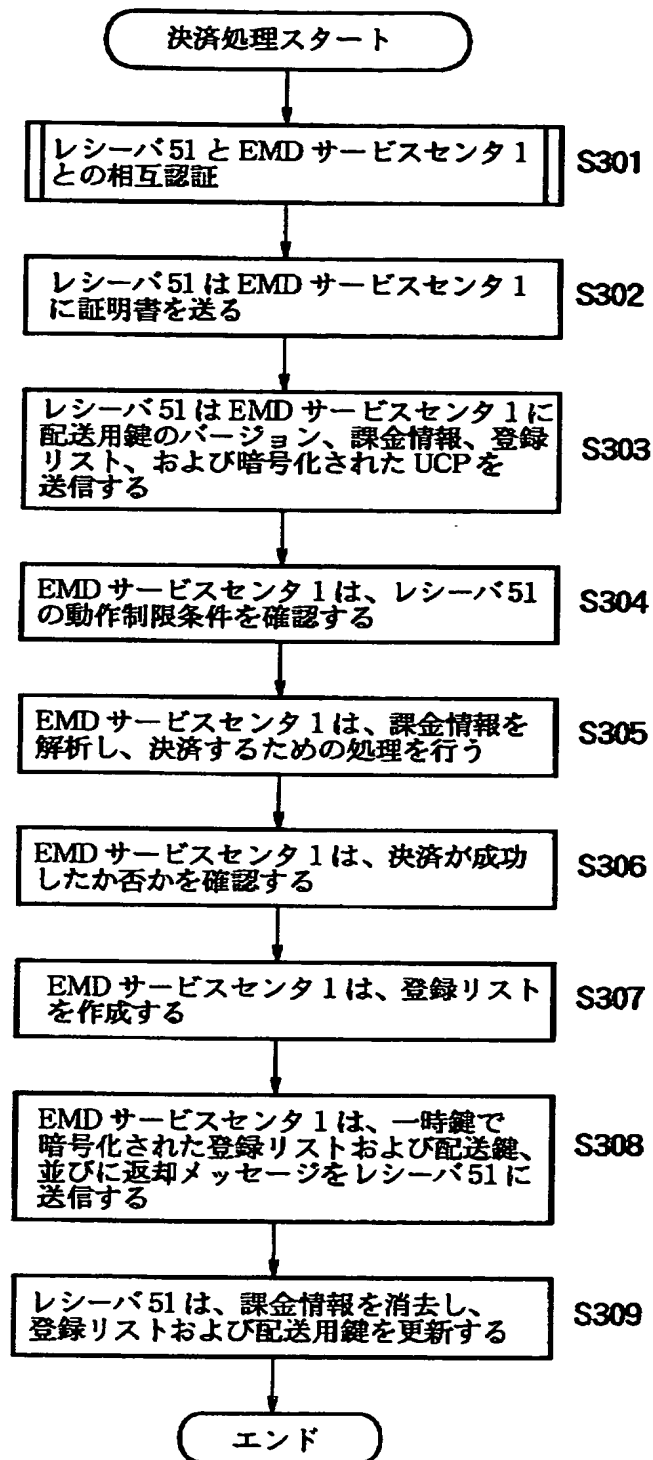
【図 40】



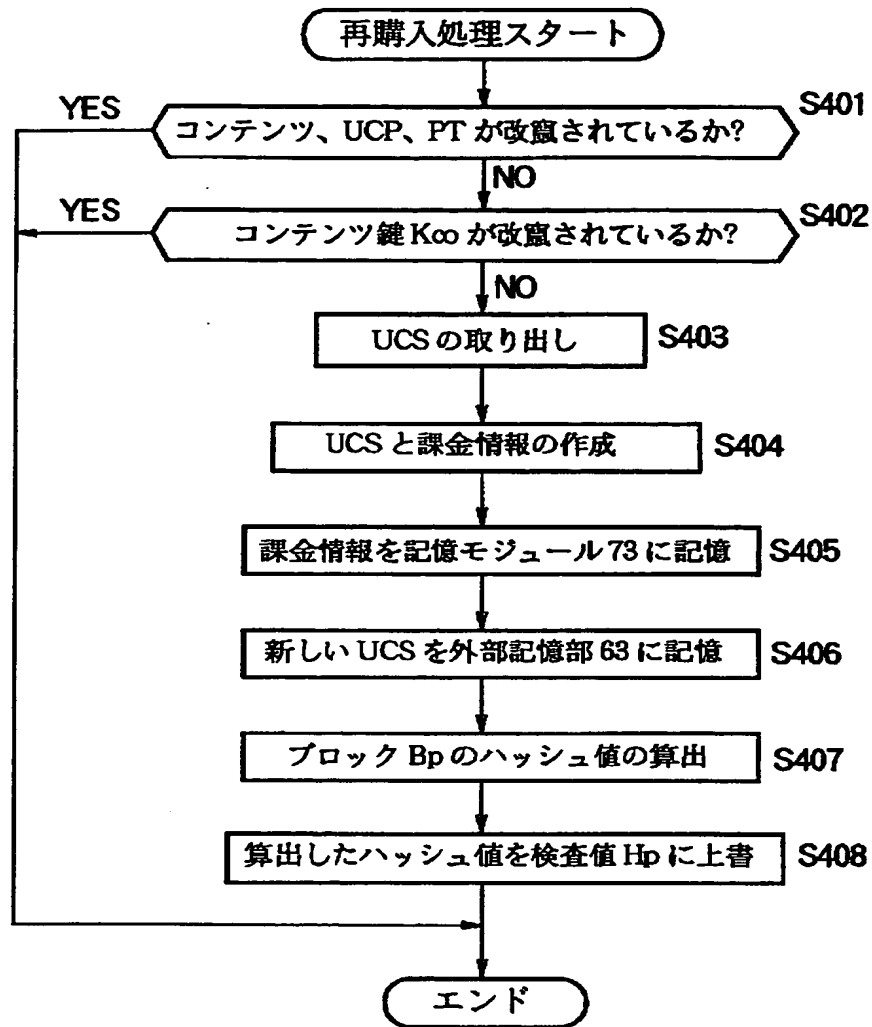
【図 4 1】



【図 4 2】



【図 4 3】



【図 4 4】

コンテンツの ID		コンテンツ A の ID
コンテンツ プロバイダの ID		コンテンツプロバイダ 2 の ID
UCP の ID		ucpA の ID
UCP の有効期限		ucpA の有効期限
サービス プロバイダの ID		サービスプロバイダ 3 の ID
PT の ID		ptA-1 の ID
PT の有効期限		ptA-1 の有効期限
UCS の ID		ucsA の ID
SAM の ID		SAM62 の ID
ユーザの ID		ユーザ F の ID
利用 内容	ID	利用内容 15 の ID
	形式	形式 13→形式 11
	パラメータ	×××
	管理移動 状態情報	管理移動元：SAM62 の ID、 管理移動先：SAM62 の ID
利用履歴		×××

UCSB

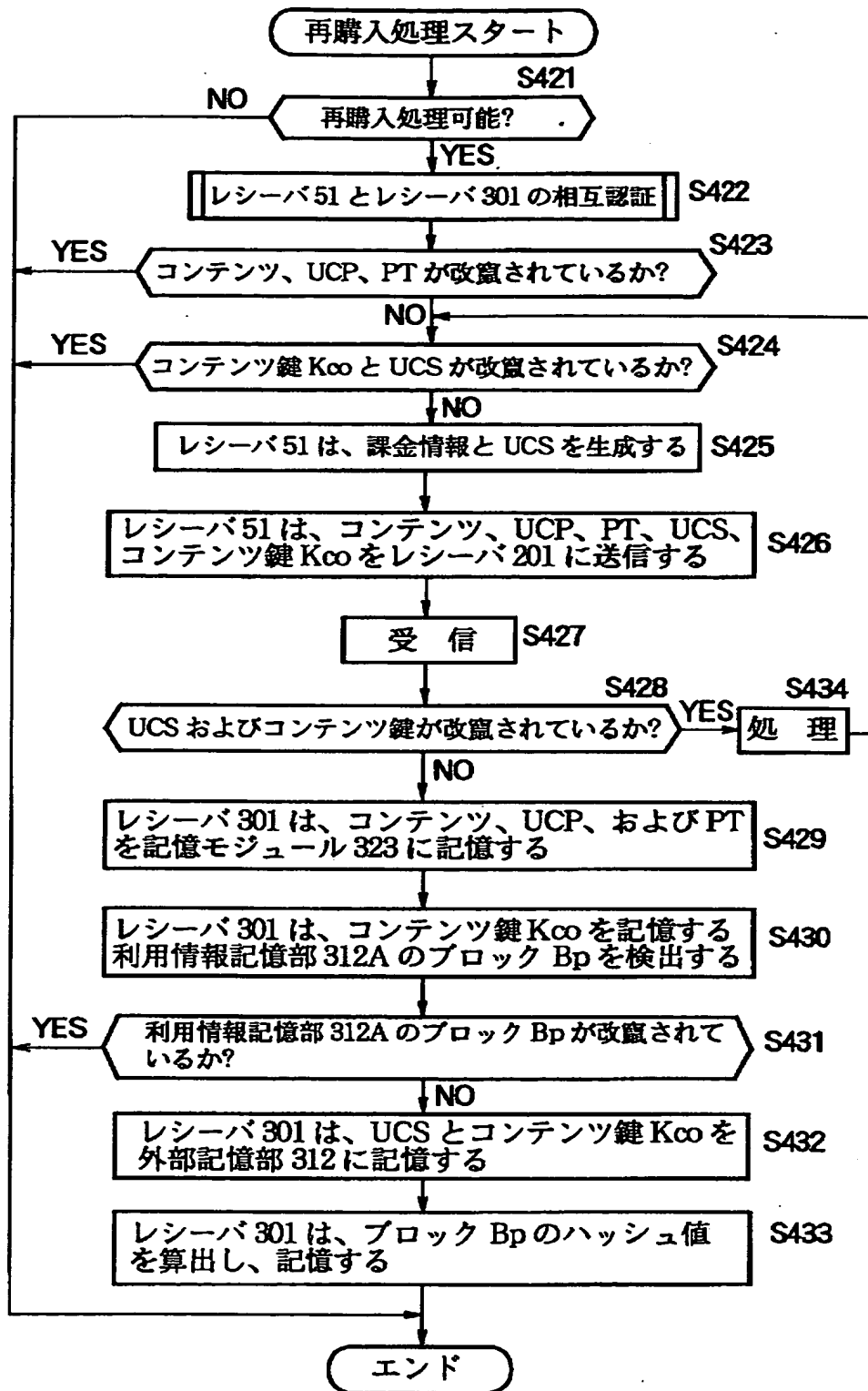
【図 4 5】

コンテンツの ID		コンテンツ A の ID
コンテンツ プロバイダの ID		コンテンツプロバイダ 2 の ID
UCP の ID		ucpA の ID
UCP の有効期限		ucpA の有効期限
サービス プロバイダの ID		サービスプロバイダ 3 の ID
PT の ID		PTA-1 の ID
PT の有効期限		PTA-1 の有効期限
UCS の ID		ucsA の ID
SAM の ID		SAM62 の ID
ユーザの ID		ユーザ F の ID
利用 内容	ID	利用内容 15 の ID
	形式	形式 13→形式 11
	パラメータ	×××
	管理移動 状態情報	管理移動元：SAM62 の ID、 管理移動先：SAM62 の ID

課金情報 B



【図 4 6】



【図 4 7】

コンテンツの ID		コンテンツ A の ID
コンテンツ プロバイダの ID		コンテンツプロバイダ 2 の ID
UCP の ID		ucpA の ID
UCP の有効期限		ucpA の有効期限
サービス プロバイダの ID		サービスプロバイダ 3 の ID
PT の ID		ptA-1 の ID
PT の有効期限		ptA-1 の有効期限
UCS の ID		ucsA の ID
SAM の ID		SAM62 の ID
ユーザの ID		ユーザ F の ID
利用 内容	ID	利用内容 16 の ID
	形式	形式 11→形式 11
	パラメータ	×××
	管理移動 状態情報	管理移動元：SAM62 の ID、 管理移動先：SAM62 の ID
利用履歴		×××

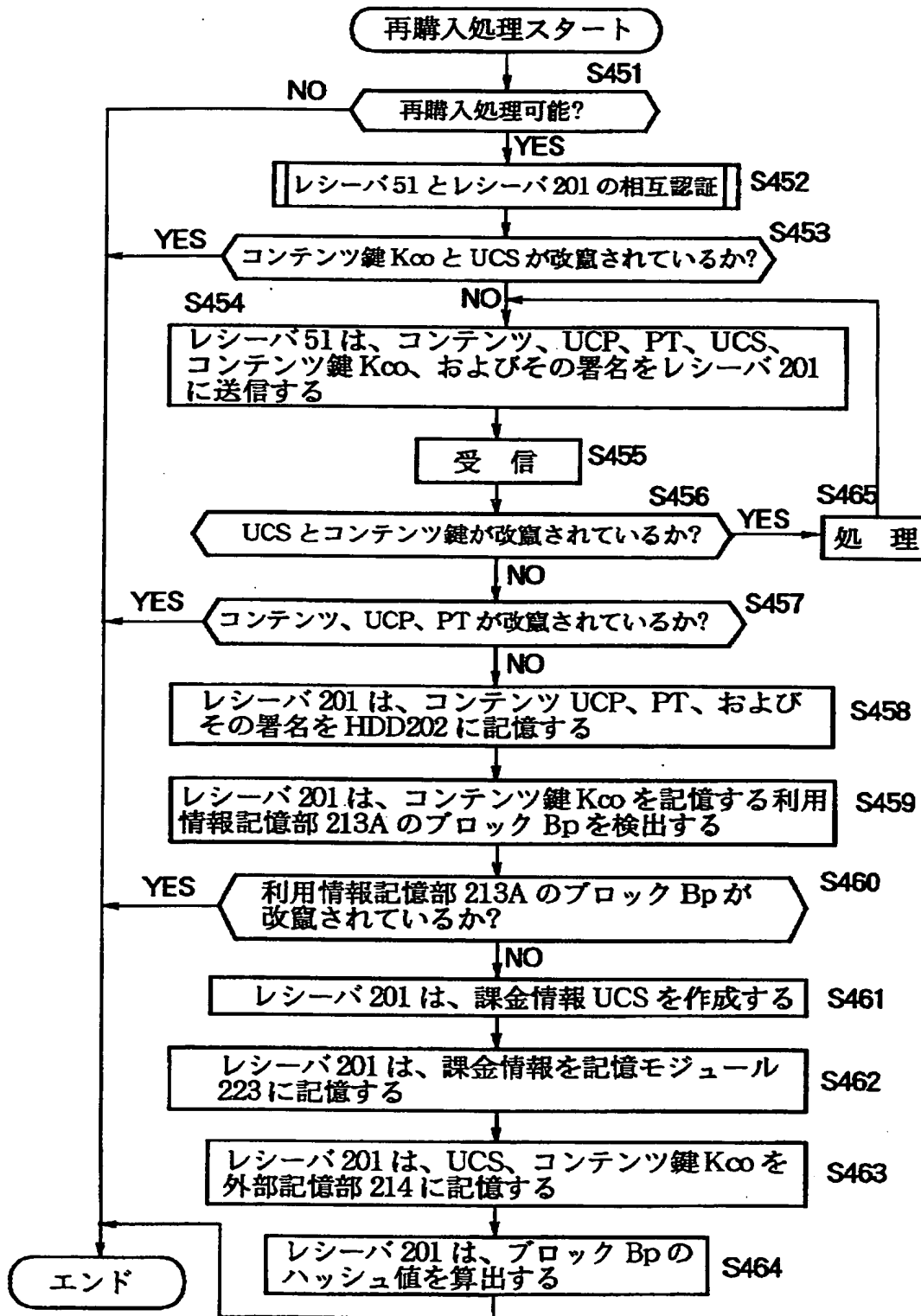
UCSC

【図 4 8】

コンテンツの ID		コンテンツ A の ID
コンテンツ プロバイダの ID		コンテンツプロバイダ 2 の ID
UCP の ID		ucpA の ID
UCP の有効期限		ucpA の有効期限
サービス プロバイダの ID		サービスプロバイダ 3 の ID
PT の ID		PTA-1 の ID
PT の有効期限		PTA-1 の有効期限
UCS の ID		ucsA の ID
SAM の ID		SAM62 の ID
ユーザの ID		ユーザ F の ID
利用 内容	ID	利用内容 16 の ID
	形式	形式 11 → 形式 11
	パラメータ	× × ×
	管理移動 状態情報	管理移動元：SAM62 の ID、 管理移動先：SAM62 の ID

課金情報 C

【図 4 9】



【図 50】

コンテンツの ID		コンテンツ A の ID
コンテンツ プロバイダの ID		コンテンツプロバイダ 2 の ID
UCP の ID		ucpA の ID
UCP の有効期限		ucpA の有効期限
サービス プロバイダの ID		サービスプロバイダ 3 の ID
PT の ID		ptA-1 の ID
PT の有効期限		ptA-1 の有効期限
UCS の ID		ucsA の ID
SAM の ID		SAM212 の ID
ユーザの ID		ユーザ F の ID
利用 内容	ID	利用内容 16 の ID
	形式	形式 11→形式 11
	パラメータ	×××
	管理移動 状態情報	管理移動元：SAM62 の ID、 管理移動先：SAM62 の ID
利用履歴		×××

ucsD

【図 5 1】

コンテンツの ID		コンテンツ A の ID
コンテンツ プロバイダの ID		コンテンツプロバイダ 2 の ID
UCP の ID		UCPA の ID
UCP の有効期限		UCPA の有効期限
サービス プロバイダの ID		サービスプロバイダ 3 の ID
PT の ID		PTA-1 の ID
PT の有効期限		PTA-1 の有効期限
UCS の ID		UCSA の ID
SAM の ID		SAM212 の ID
ユーザの ID		ユーザ F の ID
利用 内容	ID	利用内容 16 の ID
	形式	形式 11→形式 11
	パラメータ	×××
	管理移動 状態情報	管理移動元：SAM62 の ID、 管理移動先：SAM62 の ID

課金情報 D

【書類名】 要約書

【要約】

【課題】 一度購入したコンテンツを再購入する場合、割引価格で、それを購入することができるようにする。

【解決手段】 コンテンツを再購入する場合、そのとき作成される課金情報 B の「課金履歴」には”割引価格”が設定される。”割引価格”が「課金履歴」に設定された課金情報に基づいて、決済が行われるので、コンテンツを再購入するユーザは、割引価格で、それを購入することができる。

【選択図】 図 4 5

出 願 人 履 歴 情 報

識別番号 [000002185]

1. 変更年月日 1990年 8月30日  
[変更理由] 新規登録  
住 所 東京都品川区北品川6丁目7番35号  
氏 名 ソニー株式会社



## 明 細 書

情報処理装置および方法、並びに提供媒体

### 技術分野

本発明は、情報処理装置および方法、並びに提供媒体に関し、特に、暗号化された情報を利用する情報処理装置および方法、並びに提供媒体に関する。

### 背景技術

音楽などの情報（以下、コンテンツと称する）を暗号化し、所定の契約を交わしたユーザの情報処理装置に送信し、ユーザが、情報処理装置でコンテンツを復号して、利用するシステムがある。

ユーザが複数の情報処理装置を有している場合、そのユーザは、それぞれの情報処理装置毎に、コンテンツを購入し、その利用料金を支払わなければならない。すなわち、一度購入したコンテンツであっても、異なる情報処理装置においてそれを利用する場合（購入する場合）、同一の料金で、再度購入する必要がある。

### 発明の開示

本発明はこのような状況に鑑みてなされたものであり、同一のコンテンツを再購入する場合、ユーザが、割引料金で、購入することができるようにするものである。

かかる課題を解決するため本発明においては、情報処理装置において、購入した権利の内容を示す第 1 の利用内容、および第 1 の利用内容に対応する価格内容を特定する第 1 の使用許諾条件情報を作成する第 1 の作成手段と、暗号化されている情報、第 1 の使用許諾条件情報、購入した権利の内容に基づいて再購入することができる権利の内容を示す第 2 の利用形式を含む取扱方針、第 2 の利用内容

に対応する価格内容を含む価格情報、および暗号化されている情報を復号するために必要な鍵を記憶する記憶手段と、他の情報処理装置を介して、権利の再購入が行われるとき、取扱方針と価格情報に基づいて、第2の利用内容、および第2の利用内容に対応する価格内容を特定する第2の使用許諾条件情報を作成する第2の作成手段と、第2の作成手段により作成された第2の使用許諾条件情報、並びに記憶手段に記憶されている、暗号化されている情報および鍵を、他の情報処理装置に送信する送信手段とを具備する。

また本発明においては、情報処理方法において、購入した権利の内容を示す第1の利用内容、および第1の利用内容に対応する価格内容を特定する第1の使用許諾条件情報を作成する第1の作成ステップと、暗号化されている情報、第1の使用許諾条件情報、購入した権利の内容に基づいて再購入することができる権利の内容を示す第2の利用形式を含む取扱方針、第2の利用内容に対応する価格内容を含む価格情報、および暗号化されている情報を復号するために必要な鍵を記憶する記憶ステップと、他の情報処理装置を介して、権利の再購入が行われるとき、取扱方針と価格情報に基づいて、第2の利用内容、および第2の利用内容に対応する価格内容を特定する第2の使用許諾条件情報を作成する第2の作成ステップと、第2の作成ステップで作成された第2の使用許諾条件情報、並びに記憶ステップに記憶されている、暗号化されている情報および鍵を、他の情報処理装置に送信する送信ステップとを具備する。

さらに本発明においては、提供媒体において、購入した権利の内容を示す第1の利用内容、および第1の利用内容に対応する価格内容を特定する第1の使用許諾条件情報を作成する第1の作成ステップと、暗号化されている情報、第1の使用許諾条件情報、購入した権利の内容に基づいて再購入することができる権利の内容を示す第2の利用形式を含む取扱方針、第2の利用内容に対応する価格内容を含む価格情報、および暗号化されている情報を復号するために必要な鍵を記憶する記憶ステップと、他の情報処理装置を介して、権利の再購入が行われるとき、取扱方針と価格情報に基づいて、第2の利用内容、および第2の利用内容に対

応する価格内容を特定する第2の使用許諾条件情報を作成する第2の作成ステップと、第2の作成ステップで作成された第2の使用許諾条件情報、並びに記憶ステップに記憶されている、暗号化されている情報および鍵を、他の情報処理装置に送信する送信ステップとを具備する処理を実行させるコンピュータが読み取り可能なプログラムを提供する。

さらに本発明においては、情報処理装置、情報処理方法、提供媒体において、購入された権利の内容を示す第1の利用内容、および第1の利用内容に対応する価格内容を特定する第1の使用許諾条件情報が作成され、暗号化されている情報、第1の使用許諾条件情報、購入した権利の内容に基づいて再購入することができる権利の内容を示す第2の利用形式を含む取扱方針、第2の利用内容に対応する価格内容を含む価格情報、および暗号化されている情報を復号するために必要な鍵が記憶され、他の情報処理装置を介して、権利の再購入が行われるとき、取扱方針と価格情報に基づいて、第2の利用内容、および第2の利用内容に対応する価格内容を特定する第2の使用許諾条件情報が作成され、作成された第2の使用許諾条件情報、並びに記憶手段に記憶されている、暗号化されている情報および鍵が、他の情報処理装置に送信される。

さらに本発明においては、情報処理装置において、他の情報処理装置から送信されてきた、暗号化されている情報、暗号化されている情報を復号するために必要な鍵、および権利の内容を示す利用内容と利用内容に対応する価格内容を特定する使用許諾条件情報を受信する受信手段と、使用許諾条件情報により特定される利用内容に示される権利の内容に基づいて、情報を利用するための処理を実行する実行手段とを具備する。

さらに本発明においては、情報処理方法において、他の情報処理装置から送信されてきた、暗号化されている情報、暗号化されている情報を復号するために必要な鍵、および権利の内容を示す利用内容と利用内容に対応する価格内容を特定する使用許諾条件情報を受信する受信ステップと、使用許諾条件情報により特定される利用内容に示される権利の内容に基づいて、情報を利用するための処理を

実行する実行ステップとを具備する。

さらに本発明においては、提供媒体において、他の情報処理装置から送信されてきた、暗号化されている情報、暗号化されている情報を復号するために必要な鍵、および権利の内容を示す利用内容と利用内容に対応する価格内容を特定する使用許諾条件情報を受信する受信ステップと、使用許諾条件情報により特定される利用内容に示される権利の内容に基づいて、情報を利用するための処理を実行する実行ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供する。

さらに本発明においては、情報処理装置、情報処理方法、提供媒体において、他の情報処理装置から送信されてきた、暗号化されている情報、暗号化されている情報を復号するために必要な鍵、および権利の内容を示す利用内容と利用内容に対応する価格内容を特定する使用許諾条件情報が受信され、使用許諾条件情報により特定される利用内容に示される権利の内容に基づいて、情報を利用するための処理が実行される。

さらに本発明においては、情報処理装置において、暗号化されている情報、購入することができる権利の内容を示す利用内容を含む取扱方針、利用内容に対応する価格内容を含む価格情報、および暗号化されている情報を復号するために必要な鍵を記憶する記憶手段と、記憶手段に記憶されている取扱方針および価格情報に基づいて、利用内容、および利用内容に対応する価格内容を特定する使用許諾条件情報を作成する作成手段と、他の情報処理装置において、権利の再購入が行われるとき、作成手段により作成された使用許諾条件情報、並びに記憶手段に記憶されている、暗号化されている情報および鍵を、他の情報処理装置に送信する送信手段とを具備する。

さらに本発明においては、情報処理方法において、暗号化されている情報、購入することができる権利の内容を示す利用内容を含む取扱方針、利用内容に対応する価格内容を含む価格情報、および暗号化されている情報を復号するために必要な鍵を記憶する記憶ステップと、記憶ステップで記憶された取扱方針および価

格情報に基づいて、利用内容、および利用内容に対応する価格内容を特定する使用許諾条件情報を作成する作成ステップと、他の情報処理装置において、権利の再購入が行われるとき、作成ステップで作成された使用許諾条件情報、並びに記憶ステップで記憶された、暗号化されている情報および鍵を、他の情報処理装置に送信する送信ステップとを具備する。

さらに本発明においては、提供媒体において、暗号化されている情報、購入することができる権利の内容を示す利用内容を含む取扱方針、利用内容に対応する価格内容を含む価格情報、および暗号化されている情報を復号するために必要な鍵を記憶する記憶ステップと、記憶ステップで記憶された取扱方針および価格情報に基づいて、利用内容、および利用内容に対応する価格内容を特定する使用許諾条件情報を作成する作成ステップと、他の情報処理装置において、権利の再購入が行われるとき、作成ステップで作成された使用許諾条件情報、並びに記憶ステップで記憶された、暗号化されている情報および鍵を、他の情報処理装置に送信する送信ステップとを具備する処理を実行させるコンピュータが読み取り可能なプログラムを提供する。

さらに本発明においては、情報処理装置、情報処理方法、提供媒体において、暗号化されている情報、購入することができる権利の内容を示す利用内容を含む取扱方針、利用内容に対応する価格内容を含む価格情報、および暗号化されている情報を復号するために必要な鍵が記憶され、記憶された取扱方針および価格情報に基づいて、利用内容、および利用内容に対応する価格内容を特定する使用許諾条件情報が作成され、他の情報処理装置において、権利の再購入が行われるとき、作成された使用許諾条件情報、並びに記憶された、暗号化されている情報および鍵が、他の情報処理装置に送信される。

さらに本発明においては、情報処理装置において、他の情報処理装置から送信されてきた、暗号化されている情報、暗号化されている情報を復号するために必要な鍵、および所定の権利の内容を示す第1の利用形式、および第1の利用形式に対応する価格内容を特定する使用許諾条件情報を受信する受信手段と、受信手

段により受信された使用許諾条件情報により特定される第 1 の利用内容に示される権利の内容に基づて再購入される権利の内容を示す第 2 の利用内容を含む取扱方針、および第 2 の利用内容に対応する価格内容を含む価格情報を記憶する記憶手段と、記憶手段に記憶されている取扱方針および価格情報に基づいて、第 2 の利用内容、および第 2 の利用内容に対応する価格内容を特定する第 2 の使用許諾条件情報を作成する第 1 の作成手段とを具備する。

さらに本発明においては、情報処理方法において、他の情報処理装置から送信されてきた、暗号化されている情報、暗号化されている情報を復号するために必要な鍵、および所定の権利の内容を示す第 1 の利用形式、および第 1 の利用形式に対応する価格内容を特定する使用許諾条件情報を受信する受信ステップと、受信ステップで受信された使用許諾条件情報により特定される第 1 の利用内容に示される権利の内容に基づて再購入される権利の内容を示す第 2 の利用内容を含む取扱方針、および第 2 の利用内容に対応する価格内容を含む価格情報を記憶する記憶ステップと、記憶ステップで記憶された取扱方針および価格情報に基づいて、第 2 の利用内容、および第 2 の利用内容に対応する価格内容を特定する第 2 の使用許諾条件情報を作成する作成ステップとを具備する。

さらに本発明においては、提供媒体において、他の情報処理装置から送信されてきた、暗号化されている情報、暗号化されている情報を復号するために必要な鍵、および所定の権利の内容を示す第 1 の利用形式、および第 1 の利用形式に対応する価格内容を特定する使用許諾条件情報を受信する受信ステップと、受信ステップで受信された使用許諾条件情報により特定される第 1 の利用内容に示される権利の内容に基づて再購入される権利の内容を示す第 2 の利用内容を含む取扱方針、および第 2 の利用内容に対応する価格内容を含む価格情報を記憶する記憶ステップと、記憶ステップで記憶された取扱方針および価格情報に基づいて、第 2 の利用内容、および第 2 の利用内容に対応する価格内容を特定する第 2 の使用許諾条件情報を作成する作成ステップとを具備する処理を実行させるコンピュータが読み取り可能なプログラムを提供する。

さらに本発明においては、情報処理装置、情報処理方法、提供媒体において、他の情報処理装置から送信されてきた、暗号化されている情報、暗号化されている情報を復号するために必要な鍵、および所定の権利の内容を示す第1の利用形式、および第1の利用形式に対応する価格内容を特定する使用許諾条件情報が受信され、受信された使用許諾条件情報により特定される第1の利用内容に示される権利の内容に基づいて再購入される権利の内容を示す第2の利用内容を含む取扱方針、および第2の利用内容に対応する価格内容を含む価格情報が記憶され、記憶された取扱方針および価格情報に基づいて、第2の利用内容、および第2の利用内容に対応する価格内容を特定する第2の使用許諾条件情報が作成される。

#### 図面の簡単な説明

図1は、EMDシステムを説明する系統図である。

図2は、EMDシステムにおける、主な情報の流れを説明する系統図である。

図3は、EMDサービスセンタ1の機能的構成を示すブロック図である。

図4は、EMDサービスセンタ1の配送用鍵K dの送信を説明する略線図である。

図5は、EMDサービスセンタ1の配送用鍵K dの送信を説明する他の略線図である。

図6は、EMDサービスセンタ1の配送用鍵K dの送信を説明する他の略線図である。

図7は、EMDサービスセンタ1の配送用鍵K dの送信を説明する他の略線図である。

図8は、システム登録情報の例を説明する図表である。

図9は、コンテンツプロバイダ2の機能的構成例を示すブロック図である。

図10は、UCPの例を示す図表である。

図11は、コンテンツの管理移動を説明する略線図である。

図12は、第1世代複製を説明する略線図である。

図 1 3 は、コンテンツプロバイダセキュアコンテナの例を示す略線図である。

図 1 4 は、コンテンツプロバイダ 2 の証明書の例を示す略線図である。

図 1 5 は、サービスプロバイダ 3 の機能的構成を示すブロック図である。

図 1 6 は、P T の例を示す図表である。

図 1 7 は、サービスプロバイダセキュアコンテナの例を示す略線図である。

図 1 8 は、サービスプロバイダ 3 の証明書の例を示す略線図である。

図 1 9 は、ユーザホームネットワーク 5 のレシーバ 5 1 の機能的構成例を示すブロック図である。

図 2 0 は、レシーバ 5 1 の S A M 6 2 の証明書の例を示す略線図である。

図 2 1 は、U C S の例を示す図表である。

図 2 2 は、レシーバ 5 1 の外部記憶部 6 3 の利用情報記憶部 6 3 A の内部を説明する略線図である。

図 2 3 は、課金情報の例を示す図表である。

図 2 4 は、レシーバ 5 1 の記憶モジュール 7 3 に記憶されている情報を示す図表である。

図 2 5 は、基準情報 5 1 を説明する図表である。

図 2 6 は、レシーバ 5 1 の登録リストの例を示す図表である。

図 2 7 は、ユーザホームネットワーク 5 のレシーバ 2 0 1 の機能的構成例を示すブロック図である。

図 2 8 は、基準情報 5 1 を説明する図表である。

図 2 9 は、レシーバ 2 0 1 の登録リストの例を示す図表である。

図 3 0 は、ユーザホームネットワーク 5 のレシーバ 3 0 1 の機能的構成例を示すブロック図である。

図 3 1 は、基準情報 3 0 1 を説明する図表である。

図 3 2 は、レシーバ 3 0 1 の登録リストの例を示す図表である。

図 3 3 は、コンテンツの利用処理を説明するフローチャートである。

図 3 4 は、E M D サービスセンタ 1 がコンテンツプロバイダ 2 へ配送用鍵 K d



を送信する処理を説明するフローチャートである。

図35は、コンテンツプロバイダ2とEMDサービスセンタ1との相互認証の動作を説明するフローチャートである。

図36は、コンテンツプロバイダ2とEMDサービスセンタ1との相互認証の他の動作を説明するフローチャートである。

図37は、コンテンツプロバイダ2とEMDサービスセンタ1との相互認証の他の動作を説明するフローチャートである。

図38は、コンテンツプロバイダ2がサービスプロバイダ3にコンテンツプロバイダセキュアコンテナを送信する処理を説明するフローチャートである。

図39は、サービスプロバイダ3がレシーバ51にサービスプロバイダセキュアコンテナを送信する処理を説明するフローチャートである。

図40は、レシーバ51がサービスプロバイダセキュアコンテナを受信する処理を説明するフローチャートである。

図41は、レシーバ51がコンテンツを再生する処理を説明するフローチャートである。

図42は、課金を決済する処理を説明するフローチャートである。

図43は、再購入処理を説明するフローチャートである。

図44は、他のUCSの例を示す図表である。

図45は、他の課金情報の例を示す図表である。

図46は、他の再購入処理を説明するフローチャートである。

図47は、他のUCSの例を示す図表である。

図48は、他の課金情報の例を示す図表である。

図49は、他の再購入処理を説明するフローチャートである。

図50は、他のUCSの例を示す図表である。

図51は、他の課金情報の例を示す図表である。

発明を実施するための最良の形態

以下に本発明の実施の形態を説明する。

### (1) 情報配信システム

図1は、本発明を適用したEMD (Electronic Music Distribution: 電子音楽配信) システムを説明する図である。EMDシステムは、各装置を管理するEMDサービスセンタ1、コンテンツを提供するコンテンツプロバイダ2、コンテンツに対応する所定のサービスを提供するサービスプロバイダ3、およびコンテンツが利用される機器(この例の場合、レシーバ51、レシーバ201、およびレシーバ301)からなるユーザネットワーク5から構成されている。

EMDシステムにおけるコンテンツ(Content)とは、情報そのものが価値を有するデジタルデータで、この例の場合、1つのコンテンツは、1曲分の音楽データに相当する。尚、コンテンツは、音楽データだけでなく、映像データ、ゲームプログラム、コンピュータプログラム、著作データなどの場合も有りうる。

EMDサービスセンタ1は、EMDシステムにおける主な情報の流れを示す図2に示すように、ユーザホームネットワーク5およびコンテンツプロバイダ2に、コンテンツを利用するために必要な配送用鍵Kdを送信する。EMDサービスセンタ1はまた、ユーザホームネットワーク5の機器から、課金情報等を受信して、料金を精算する処理などを実行する。

コンテンツプロバイダ2は、提供するコンテンツ(コンテンツ鍵Kcoで暗号化されている)、そのコンテンツを復号するために必要なコンテンツ鍵Kco(配送用鍵Kdで暗号化されている)、およびコンテンツの利用内容などを示す取扱方針(以下、UCP(Usage Control Policy)と記述する)を保持し、それらを、コンテンツプロバイダセキュアコンテナ(後述)と称する形態で、サービスプロバイダ3に供給する。

サービスプロバイダ3は、コンテンツプロバイダ2から供給されるUCPの利用内容に対応して、1つまたは複数の価格情報(以下、PT(Price

T a g) と記述する) を作成する。サービスプロバイダ 3 は、作成した P T を、コンテンツプロバイダ 2 から供給されたコンテンツ (コンテンツ鍵 K c o で暗号化されている)、コンテンツ鍵 K c o (配送用鍵 K d で暗号化されている)、および U C P とともに、サービスプロバイダセキュアコンテナと称する形態で、専用のケーブルネットワーク、インターネット、または衛星通信などから構成されるネットワーク 4 を介して、ユーザホームネットワーク 5 に送信する。

ユーザホームネットワーク 5 は、供給された U C P および P T に基づいて、使用許諾条件情報 (以下、U C S (U s a g e C o n t r o l S t a t u s) と称する) を作成し、作成した U C S に基づいてコンテンツを利用する処理を実行する。ユーザホームネットワーク 5 はまた、U C S を作成するタイミングで課金情報を作成し、例えば、配送用鍵 K d の供給を受けるタイミングで、対応する U C P および P T などとともに E M D サービスセンタ 1 に送信する。

## (2) EMD サービスセンタ

図 3 は、EMD サービスセンタ 1 の機能的構成を示すブロック図である。サービスプロバイダ管理部 1 1 は、サービスプロバイダ 3 に利益分配の情報を供給する。コンテンツプロバイダ管理部 1 2 は、コンテンツプロバイダ 2 に配送用鍵 K d を送信したり、利益分配の情報を供給する。

著作権管理部 1 3 は、ユーザホームネットワーク 5 のコンテンツの利用の実績を示す情報を、著作権を管理する団体、例えば、J A S R A C ( J a p a n e s e S o c i e t y f o r R i g h t s o f A u t h o r s , C o m p o s e r s a n d P u b l i s h e r s : 日本音楽著作権協会) に送信する。

鍵サーバ 1 4 は、配送用鍵 K d を記憶しており、それを、コンテンツプロバイダ管理部 1 2 を介してコンテンツプロバイダ 2 に供給したり、ユーザ管理部 1 8 等を介してユーザホームネットワーク 5 に供給する。

ユーザホームネットワーク 5 の機器およびコンテンツプロバイダ 2 に供給される、EMD サービスセンタ 1 からの配送用鍵 K d について、図 4 乃至図 7 を参照

して説明する。

図4は、コンテンツプロバイダ2がコンテンツの提供を開始し、ユーザホームネットワーク5を構成するレシーバ51がコンテンツの利用を開始する、1998年1月における、EMDサービスセンタ1が有する配送用鍵Kd、コンテンツプロバイダ2が有する配送用鍵Kd、およびレシーバ51が有する配送用鍵Kdを示す図である。

図4の例において、配送用鍵Kdは、暦の月の初日から月の末日まで、使用可能であり、たとえば、所定のビット数の乱数である”aaaaaaaa”の値を有するバージョン1である配送用鍵Kdは、1998年1月1日から1998年1月31日まで使用可能（すなわち、1998年1月1日から1998年1月31日の期間にサービスプロバイダ3を介してユーザホームネットワーク5に配布されるコンテンツを暗号化するコンテンツ鍵Kcoは、バージョン1である配送用鍵Kdで暗号化されている）であり、所定のビット数の乱数である”bbbbbbbb”の値を有するバージョン2である配送用鍵Kdは、1998年2月1日から1998年2月28日まで使用可能（すなわち、その期間にサービスプロバイダ3を介してユーザホームネットワーク5に配布されるコンテンツを暗号化するコンテンツ鍵Kcoは、バージョン2である配送用鍵Kdで暗号化されている）である。同様に、バージョン3である配送用鍵Kdは、1998年3月中に使用可能であり、バージョン4である配送用鍵Kdは、1998年4月中に使用可能であり、バージョン5である配送用鍵Kdは、1998年5月中に使用可能であり、バージョン6である配送用鍵Kdは、1998年6月中に使用可能である。

コンテンツプロバイダ2がコンテンツの提供を開始するに先立ち、EMDサービスセンタ1は、コンテンツプロバイダ2に、1998年1月から1998年6月まで利用可能な、バージョン1乃至バージョン6の6つの配送用鍵Kdを送信し、コンテンツプロバイダ2は、6つの配送用鍵Kdを受信し、記憶する。6ヶ月分の配送用鍵Kdを記憶するのは、コンテンツプロバイダ2が、コンテンツを

提供する前のコンテンツおよびコンテンツ鍵の暗号化などの準備に、所定の期間が必要だからである。

また、レシーバ51がコンテンツの利用を開始するに先立ち、EMDサービスセンタ1は、レシーバ51に、1998年1月から1998年3月まで、利用可能なバージョン1乃至バージョン3である3つの配送用鍵Kdを送信し、レシーバ51は、3つの配送用鍵Kdを受信し、記憶する。3ヶ月分の配送用鍵Kdを記憶するのは、レシーバ51が、EMDサービスセンタ1に接続できないなどのトラブルにより、コンテンツの利用が可能な契約期間にもかかわらずコンテンツが利用できない等の事態を避けるためであり、また、EMDサービスセンタ1への接続の頻度を低くし、ユーザホームネットワーク5の負荷を低減するためである。

1998年1月1日から1998年1月31日の期間には、バージョン1である配送用鍵Kdが、EMDサービスセンタ1、コンテンツプロバイダ2、ユーザホームネットワーク5を構成するレシーバ51で利用される。

1998年2月1日における、EMDサービスセンタ1の配送用鍵Kdのコンテンツプロバイダ2、およびレシーバ51への送信を図5で説明する。EMDサービスセンタ1は、コンテンツプロバイダ2に、1998年2月から1998年7月まで利用可能な、バージョン2乃至バージョン7の6つの配送用鍵Kdを送信し、コンテンツプロバイダ2は、6つの配送用鍵Kdを受信し、受信前に記憶していた配送用鍵Kdに上書きし、新たな配送用鍵Kdを記憶する。EMDサービスセンタ1は、レシーバ51に、1998年2月から1998年4月まで、利用可能なバージョン2乃至バージョン4である3つの配送用鍵Kdを送信し、レシーバ51は、3つの配送用鍵Kdを受信し、受信前に記憶していた配送用鍵Kdに上書きし、新たな配送用鍵Kdを記憶する。EMDサービスセンタ1は、バージョン1である配送用鍵Kdをそのまま記憶する。これは、不測のトラブルが発生したとき、若しくは不正が発生し、または発見されたときに、過去に利用した配送用鍵Kdを利用できるようにするためである。

1998年2月1日から1998年2月28日の期間には、バージョン2である配送用鍵Kdが、EMDサービスセンタ1、コンテンツプロバイダ2、ユーザホームネットワーク5を構成するレシーバ51で利用される。

1998年3月1日における、EMDサービスセンタ1の配送用鍵Kdのコンテンツプロバイダ2、およびレシーバ51への送信を図6で説明する。EMDサービスセンタ1は、コンテンツプロバイダ2に、1998年3月から1998年8月まで利用可能な、バージョン3乃至バージョン8の6つの配送用鍵Kdを送信し、コンテンツプロバイダ2は、6つの配送用鍵Kdを受信し、受信前に記憶していた配送用鍵Kdに上書きし、新たな配送用鍵Kdを記憶する。EMDサービスセンタ1は、レシーバ51に、1998年3月から1998年5月まで、利用可能なバージョン3乃至バージョン5である3つの配送用鍵Kdを送信し、レシーバ51は、3つの配送用鍵Kdを受信し、受信前に記憶していた配送用鍵Kdに上書きし、新たな配送用鍵Kdを記憶する。EMDサービスセンタ1は、バージョン1である配送用鍵Kdおよびバージョン2である配送用鍵Kdをそのまま記憶する。

1998年3月1日から1998年3月31日の期間には、バージョン3である配送用鍵Kdが、EMDサービスセンタ1、コンテンツプロバイダ2、ユーザホームネットワーク5を構成するレシーバ51で利用される。

1998年4月1日における、EMDサービスセンタ1の配送用鍵Kdのコンテンツプロバイダ2、およびレシーバ51への送信を図7で説明する。EMDサービスセンタ1は、コンテンツプロバイダ2に、1998年4月から1998年9月まで利用可能な、バージョン4乃至バージョン9の6つの配送用鍵Kdを送信し、コンテンツプロバイダ2は、6つの配送用鍵Kdを受信し、受信前に記憶していた配送用鍵Kdに上書きし、新たな配送用鍵Kdを記憶する。EMDサービスセンタ1は、レシーバ51に、1998年4月から1998年6月まで、利用可能なバージョン3乃至バージョン5である3つの配送用鍵Kdを送信し、レシーバ51は、3つの配送用鍵Kdを受信し、受信前に記憶していた配送用鍵K

dに上書きし、新たな配送用鍵K dを記憶する。EMDサービスセンタ1は、バージョン1である配送用鍵K d、バージョン2である配送用鍵K d、およびバージョン3である配送用鍵K dをそのまま記憶する。

1998年4月1日から1998年4月30日の期間には、バージョン4である配送用鍵K dが、EMDサービスセンタ1、コンテンツプロバイダ2、ユーザホームネットワーク5を構成するレシーバ51で利用される。

このように、あらかじめ先の月の配送用鍵K dを配布しておくことで、仮にユーザが1、2ヶ月まったくEMDサービスセンタ1にアクセスしていなくても、一応、コンテンツの買い取りが行え、時を見計らって、EMDサービスセンタ1にアクセスして鍵を受信することができる。

図3に戻り、経歴データ管理部15は、ユーザ管理部18から出力される、課金情報、そのコンテンツに対応するPT、およびそのコンテンツに対応するUCPなどを記憶する。

利益分配部16は、経歴データ管理部15から供給された各種情報に基づき、EMDサービスセンタ1、コンテンツプロバイダ2、およびサービスプロバイダ3の利益をそれぞれ算出し、その結果をサービスプロバイダ管理部11、コンテンツプロバイダ管理部12、出納部20、および著作権管理部13に出力する。

相互認証部17は、コンテンツプロバイダ2、サービスプロバイダ3、およびユーザホームネットワーク5の機器と相互認証を実行する。

ユーザ管理部18は、EMDシステムに登録可能な、ユーザホームネットワーク5の機器に関する情報（以下、システム登録情報と称する）を管理する。システム登録情報には、図8に示すように、「SAM (Secure Application Module) のID」、「機器番号」、「決済ID」、「決済ユーザ情報」、複数の「従属ユーザ情報」、および「利用ポイント情報」の項目に対応する情報が含まれる。

「SAMのID」には、製造された、ユーザホームネットワーク5の機器のSAM（後述）のIDが記憶される。図8のシステム登録情報の「SAMのID」

には、レシーバ51のSAM62のID、レシーバ201のSAM212のID、およびレシーバ301のSAM311のIDが設定されている。

「機器番号」には、SAMを有するユーザホームネットワーク5の機器に、予め設定された機器番号が設定されている。ユーザホームネットワーク5の機器が、ネットワーク4を介してサービスプロバイダ3と、およびEMDサービスセンタ1と直接通信することができる機能を有し（通信部を有し）、かつ、例えば、UCPやPTの内容をユーザに出力（提示）したり、ユーザがUCPの利用内容を選択することができる機能を有している（表示部および操作部を有している）場合、その機器（以下、このような機能を有する機器を主機器と称する）には、100番以上の機器番号が与えられる。機器が、そのような機能を有しない場合、その機器（以下、このような機器を従機器と称する）には、99番以下の機器番号が与えられる。この例の場合、詳細は後述するが、レシーバ51およびレシーバ201の両者は、上述した機能を有しているので、主機器とされ、対応する「機器番号」には、機器番号100番がそれぞれ設定されている。一方、レシーバ301は、上述した機能を有していないので、従機器とされ、対応する「機器番号」には、機器番号25番が設定されている。

「決済ID」には、課金を決済するユーザ（以下、決済ユーザと称する）に割り当てられた所定の決済IDが設定される。この例の場合、レシーバ51、レシーバ201、およびレシーバ301は、ユーザFが決済ユーザとされて登録されているので、それらの「決済ID」には、ユーザFの決済IDが、それぞれ設定されている。

「決済ユーザ情報」には、決済ユーザの、氏名、住所、電話番号、決済機関情報（例えば、クレジットカード番号等）、生年月日、年齢、性別、ID、パスワードなどが設定される。「決済ユーザ情報」に設定される決済ユーザの、氏名、住所、電話番号、決済機関の情報、生年月日、年齢、および性別（以下、「決済ユーザ情報」に設定されるこれらの情報を、個々に区別する必要がない場合、まとめて、ユーザ一般情報と称する）は、登録が申請される際にユーザから提供さ



れ、設定される。また、この例の場合、そのうちの、氏名、住所、電話番号、および決済機関の情報は、それらに基づいて与信処理が行われるので、正確な情報（例えば、決済機関に登録されている情報）である必要がある。それに対してユーザー一般情報の生年月日、年齢、および性別は、与信処理には用いられないので、この例の場合、それらの情報は、正確である必要はなく、またユーザは、その情報を必ずしも提供する必要がない。「決済ユーザ情報」に記憶される決済ユーザの、IDおよびパスワードは、EMDシステムに登録されるときに割り当てられ、設定される。

図8のシステム登録情報の、レシーバ51のSAM62のID、レシーバ201のSAM212のID、およびレシーバ301のSAM311のIDに対応する「決済ユーザ情報」には、ユーザFから提供されたユーザー一般情報、ユーザFのID、およびユーザFのパスワードが設定されている。

「従属ユーザ情報」には、課金を決済しないユーザ（以下、このようなユーザを従属ユーザと称する）の、氏名、住所、電話番号、生年月日、年齢、性別、ID、パスワードなどが設定される。すなわち、「決済ユーザ情報」に設定される情報のうち、決済機関の情報以外の情報が設定される。

従属ユーザに対しては与信処理が行われないので、「従属ユーザ情報」に設定される従属ユーザの、氏名、住所、電話番号、生年月日、年齢、および性別の情報は、正確なものである必要がない。例えば、氏名の場合は、ニックネームのようなものでもよい。また氏名はユーザを特定するために必要とされるが、他の情報は、ユーザは必ずしも提供する必要がない。「従属ユーザ情報」に設定される従属ユーザの、IDおよびパスワードは、登録されるときに割り当てられ、設定される。

この例の場合、レシーバ201およびレシーバ301の両者には、ユーザAが、従属ユーザとして登録されているので、図8のシステム登録情報の、レシーバ201のSAM212のIDおよびレシーバ301のSAM311のIDに対応する「従属ユーザ情報」には、ユーザAから提供されたユーザー一般情報（決済機

関情報を除く)、ユーザAのID、およびユーザAのパスワードが設定されている。レシーバ51には、従属ユーザが設けられていないので、SAM62のIDに対応する「従属ユーザ情報」には、何の情報も設定されていない。

「利用ポイント情報」には、利益分配部16から出力された利用ポイントが設定される。図8のシステム登録情報の、レシーバ51のSAM62のID、レシーバ201のSAM212のID、およびレシーバ301のSAM311のIDに対応する「利用ポイント情報」には、それぞれの利用ポイント情報が設定されている。

ユーザ管理部18は、このようなシステム登録情報を管理する他、所定の処理に対応して登録リスト（後述）を作成し、配送用鍵Kdとともにユーザホームネットワーク5に送信する。

課金請求部19は、経歴データ管理部15から供給された、例えば、課金情報、UCP、およびPTに基づき、ユーザへの課金を算出し、その結果を、出納部20に供給する。出納部20は、ユーザ、コンテンツプロバイダ2、およびサービスプロバイダ3への出金、徴収すべき利用料金の金額を基に、図示せぬ外部の銀行等と通信し、決算処理を実行する。出納部20はまた、決算処理の結果をユーザ管理部18に通知する。監査部21は、ユーザホームネットワーク5の機器から供給された課金情報、PT、およびUCPの正当性（すなわち、不正をしていないか）を監査する。

### (3) コンテンツプロバイダ

図9は、コンテンツプロバイダ2の機能的構成を示すブロック図である。コンテンツサーバ31は、ユーザに供給するコンテンツを記憶し、ウォーターマーク付加部32に供給する。ウォーターマーク付加部32は、コンテンツサーバ31から供給されたコンテンツにウォーターマーク（電子透かし）を付加し、圧縮部33に供給する。

圧縮部33は、ウォーターマーク付加部32から供給されたコンテンツを、ATRA C2 (Adaptive Transform Acoustic

Coding 2) (商標) 等の方式で圧縮し、暗号化部 34 に供給する。暗号化部 34 は、圧縮部 33 で圧縮されたコンテンツを、乱数発生部 35 から供給された乱数を鍵 (以下、この乱数をコンテンツ鍵  $K_c$  と称する) として、DES (Data Encryption Standard) などの共通鍵暗号方式で暗号化し、その結果をセキュアコンテナ作成部 38 に出力する。

乱数発生部 35 は、コンテンツ鍵  $K_c$  となる所定のビット数の乱数を暗号化部 34 および暗号化部 36 に供給する。暗号化部 36 は、コンテンツ鍵  $K_c$  を EMD サービスセンタ 1 から供給された配送用鍵  $K_d$  を使用して、DES などの共通鍵暗号方式で暗号化し、その結果をセキュアコンテナ作成部 38 に出力する。

DES は、56 ビットの共通鍵を用い、平文の 64 ビットを 1 ブロックとして処理する暗号方式である。DES の処理は、平文を攪拌し、暗号文に変換する部分 (データ攪拌部) と、データ攪拌部で使用する鍵 (拡大鍵) を共通鍵から生成する部分 (鍵処理部) からなる。DES のすべてのアルゴリズムは公開されているので、ここでは、データ攪拌部の基本的な処理を簡単に説明する。

まず、平文の 64 ビットは、上位 32 ビットの  $H_0$ 、および下位 32 ビットの  $L_0$  に分割される。鍵処理部から供給された 48 ビットの拡大鍵  $K_1$ 、および下位 32 ビットの  $L_0$  を入力とし、下位 32 ビットの  $L_0$  を攪拌した F 関数の出力が算出される。F 関数は、数値を所定の規則で置き換える「換字」およびビット位置を所定の規則で入れ替える「転置」の 2 種類の基本変換から構成されている。次に、上位 32 ビットの  $H_0$  と、F 関数の出力が排他的論理和され、その結果は  $L_1$  とされる。 $L_0$  は、 $H_1$  とされる。

上位 32 ビットの  $H_0$  および下位 32 ビットの  $L_0$  を基に、以上の処理を 16 回繰り返す、得られた上位 32 ビットの  $H_{16}$  および下位 32 ビットの  $L_{16}$  が暗号文として出力される。復号は、暗号化に使用した共通鍵を用いて、上記の手順を逆にたどることで実現される。

ポリシー記憶部 37 は、コンテンツに対応して設定される UCP を記憶し、セ

キュアコンテナ作成部 38 に出力する。図 10 は、コンテンツサーバ 31 に保持されているコンテンツ A に対応して設定され、ポリシー記憶部 37 に記憶されている UCPA を表している。UCP には、「コンテンツの ID」、「コンテンツプロバイダの ID」、「UCP の ID」、「UCP の有効期限」、「利用条件」、および「利用内容」の各項目に対応する所定の情報が含まれる。「コンテンツの ID」には、UCP が対応するコンテンツの ID が設定される。UCPA の「コンテンツの ID」には、コンテンツ A の ID が設定されている。

「コンテンツプロバイダの ID」には、コンテンツの提供元のコンテンツプロバイダの ID が設定され、UCPA の「コンテンツプロバイダの ID」には、コンテンツプロバイダ 2 の ID が設定されている。「UCP の ID」には、各 UCP に割り当てられた所定の ID が設定され、UCPA の「UCP の ID」には、UCPA の ID が設定されている。「UCP の有効期限」には、UCP の有効期限を示す情報が設定され、UCPA の「UCP の有効期限」には、UCPA の有効期限が設定されている。

「利用条件」には、「ユーザ条件」および「機器条件」の各項目に対応する所定の情報が設定される。「ユーザ条件」には、この UCP を選択することができるユーザの条件が設定され、「機器条件」には、この UCP を選択することができる機器の条件が設定される。

UCPA の場合、「利用条件 10」が設定され、「利用条件 10」の「ユーザ条件 10」には、EMD システムの利用頻度などに対応して与えられる所定の利用ポイントが 200 ポイント以上であることを示す情報（” 200 ポイント以上”）が設定されている。また「利用条件 10」の「機器条件 10」には、条件がないことを示す情報（” 条件なし”）が設定されている。すなわち、UCPA は、200 ポイント以上の利用ポイントを有するユーザのみが選択可能となる。

「利用内容」には、「ID」、「形式」、「パラメータ」、および「管理移動許可情報」の各項目に対応する所定の情報が含まれる。「ID」には、「利用内容」に設定される情報に割り当てられた所定の ID が設定される。「形式」には、再生や

複製など、コンテンツの利用形式を示す情報が設定される。「パラメータ」には、「形式」に設定された利用形式に対応する所定の情報が設定される。

「管理移動許可情報」には、コンテンツの管理移動が可能か否か（許可されているか否か）を示す情報が設定される。コンテンツの管理移動が行われると、図 1 1 (A) に示すように、管理移動元の機器にコンテンツが保持されつつ、管理移動先の機器にそのコンテンツが移動される。すなわち、管理移動元の機器と管理移動先の機器の両方において、コンテンツが利用される。この点で、図 1 1 (B) に示すように、移動元の機器にコンテンツが保持されず、移動先の機器のみにコンテンツが保持され、移動先の機器においてのみコンテンツが利用される、通常の移動とは異なる。

また、コンテンツの管理移動が行われている間、管理移動元の機器は、図 1 1 (A) に示すように、他の機器にコンテンツを管理移動することができない（許可されない）。すなわち、管理移動元の機器と管理移動先の機器の 2 機においてのみコンテンツが保持される。この点で、図 1 2 (A) に示すように、オリジナルのコンテンツから、複数の複製（第 1 世代）を作成することができる、第 1 世代の複製とも異なる。また、管理移動元の機器からコンテンツを戻すことより、他の機器にコンテンツを管理移動することができるので、この点で、図 1 2 (B) に示すように、1 回だけの複製とも異なる。

図 1 0 に戻り、UCPA には、6 つの「利用内容 1 1」乃至「利用内容 1 6」が設けられており、「利用内容 1 1」において、その「ID 1 1」には、「利用内容 1 1」に割り当てられた所定の ID が設定されている。「形式 1 1」には、コンテンツを買い取って再生する利用形式を示す情報（” 買い取り再生”）が設定される。ユーザは、” 買い取り再生” の利用形式で利用する権利を購入することより、コンテンツ A を制限なしに再生することができる。「パラメータ 1 1」には、” 買い取り再生” に対応する所定の情報が設定されている。「管理移動許可情報 1 1」には、コンテンツの管理移動が許可されていることを示す情報（” 可”）が設定されている。

「利用内容 1 2」において、その「ID 1 2」には、「利用内容 1 2」に割り当てられた所定の ID が設定されている。「形式 1 2」には、第 1 世代の複製を行う利用形式を示す情報（” 第 1 世代複製”）が設定されている。ユーザは、” 第 1 世代複製” の利用形式で利用する権利を購入することより、図 1 2（A）に示したように、オリジナルのコンテンツ A から、複数の第 1 世代の複製を作成することができる。なお、この場合、第 1 世代の複製から第 2 世代の複製を作成することはできない（許可されていない）。「パラメータ 1 2」には、” 第 1 世代複” に対応する所定の情報が設定されている。「管理移動許可情報 1 2」には、コンテンツの管理移動が許可されていないことを示す情報（” 不可”）が設定されている。

「利用内容 1 3」において、その「ID 1 3」には、「利用内容 1 3」に割り当てられた所定の ID が設定されている。「形式 1 3」には、” 期間制限再生” の利用形式が設定されている。ユーザは、” 期間制限再生” の利用形式で利用する権利を購入することより、所定の期間（時間）に限ってコンテンツ A を再生することができる。「パラメータ 1 3」には、” 期間制限再生” に対応して、その期間の開始時期（時刻）と終了時期（時刻）が設定されている。「管理移動許可情報 1 3」には、” 可” が設定されている。

「利用内容 1 4」において、その「ID 1 4」には、「利用内容 1 4」に割り当てられた所定の ID が設定されている。「形式 1 4」には、” Pay Per Copy N” の利用形式が設定されている。ユーザは、” Pay Per Copy N” の利用形式で利用する権利を購入することより、オリジナルのコンテンツ A から、N 個の複製を作成することができる（許可されている）。なお、” Pay Per Copy N” の場合も、図 1 2 の（B）に示すように、複製からの複製を作成することはできない（許可されていない）。「パラメータ 1 4」には、” Pay Per Copy N” に対応する所定の情報が設定されている。「管理移動許可情報 1 4」には、” 不可” が設定されている。

「利用内容 1 5」において、その「ID 1 5」には、「利用内容 1 5」に割り

当てられた所定のIDが設定されている。「形式15」には、「形式13→形式11」の利用形式が設定されている。ユーザは、「期限制限再生」の利用形式で利用する権利をすでに購入しているとき、この利用形式で利用する権利を購入することができ、それにより、ユーザは、コンテンツAを「買い取り再生」（形式11）で利用することができる。「パラメータ15」には、「形式13→形式11」に対応する所定の情報が設定されている。「管理移動許可情報15」には、「可」が設定されている。

「利用内容16」において、その「ID16」には、「利用内容16」に割り当てられた所定のIDが設定されている。「形式16」には、「形式11→形式11」の利用形式が設定されている。ユーザは、「買い取り再生」（形式11）の利用形式で利用する権利をすでに購入しているとき、この利用形式で利用する権利を購入することができ、それにより、ユーザは、再度、コンテンツAを「買い取り再生」で利用することができる。この利用形式で利用する権利は、例えば、レシーバ51において「買い取り再生」で利用する権利が購入され、コンテンツAが利用されているとき、レシーバ301またはレシーバ201において、コンテンツAを「買い取り再生」で利用したい場合に購入される。「パラメータ16」には、「形式11→形式11」に対応する所定の情報が設定されている。「管理移動許可情報16」には、「可」が設定されている。

図9に戻り、セキュアコンテナ作成部38は、例えば、図13に示すような、コンテンツA（コンテンツ鍵KcoAで暗号化されている）、コンテンツ鍵KcoA（配送用鍵Kdで暗号化されている）、UCPA、およびその署名からなるコンテンツプロバイダセキュアコンテナを作成する。なお、署名は、送信したいデータ（この場合、コンテンツA（コンテンツ鍵KcoAで暗号化されている））、コンテンツ鍵KcoA（配送用鍵Kdで暗号化されている）、およびUCPAの全体にハッシュ関数を適用して得られたハッシュ値が、コンテンツプロバイダの公開鍵暗号の秘密鍵（この場合、コンテンツプロバイダ2の秘密鍵Kscp）で暗号化されたものである。

セキュアコンテナ作成部 38 はまた、コンテンツプロバイダセキュアコンテナに、図 14 に示すコンテンツプロバイダ 2 の証明書を付してサービスプロバイダ 3 に送信する。この証明書は、証明書のバージョン番号、認証局がコンテンツプロバイダ 2 に対し割り付けた証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、およびコンテンツプロバイダ 2 の名前、コンテンツプロバイダ 2 の公開鍵  $K_{p\ c\ p}$ 、並びにその署名（認証局の秘密鍵  $K_{s\ c\ a}$  で暗号化されている）から構成されている。

署名は、改竄のチェックおよび作成者認証をするためのデータであり、送信したいデータを基にハッシュ関数でハッシュ値をとり、これを公開鍵暗号の秘密鍵で暗号化して作成される。

ハッシュ関数および署名の照合について説明する。ハッシュ関数は、送信したい所定のデータを入力とし、所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの 1 ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ入力データを探し出すことが困難である特徴を有する。

署名とデータを受信した受信者は、署名を公開鍵暗号の公開鍵で復号し、その結果（ハッシュ値）を得る。さらに受信されたデータのハッシュ値が計算され、計算されたハッシュ値と、署名を復号して得られたハッシュ値とが、等しいか否かが判定される。送信されたデータのハッシュ値と復号したハッシュ値が等しいと判定された場合、受信したデータは改竄されておらず、公開鍵に対応した秘密鍵を保持する送信者から送信されたデータであることがわかる。署名のハッシュ関数としては、MD (Message Digest) 4, MD 5, SHA (Secure Hash Algorithm) - 1 などが用いられる。

次に公開鍵暗号について説明する。暗号化および復号で同一の鍵（共通鍵）を使用する共通鍵暗号方式に対し、公開鍵暗号方式は、暗号化に使用する鍵と復号するときの鍵が異なる。公開鍵暗号を用いる場合、鍵の一方を公開しても他方を



秘密に保つことができ、公開しても良い鍵は、公開鍵と称され、他方の秘密に保つ鍵は、秘密鍵と称される。

公開鍵暗号の中で代表的なRSA (Rivest-Shamir-Adleman) 暗号を、簡単に説明する。まず、2つの十分に大きな素数である $p$ および $q$ を求め、さらに $p$ と $q$ の積である $n$ を求める。 $(p-1)$ と $(q-1)$ の最小公倍数 $L$ を算出し、更に、3以上 $L$ 未満で、かつ、 $L$ と互いに素な数 $e$ を求める(すなわち、 $e$ と $L$ を共通に割り切れる数は、1のみである)。

次に、 $L$ を法とする乗算に関する $e$ の乗法逆元 $d$ を求める。すなわち、 $d$ 、 $e$ 、および $L$ の間には、 $ed = 1 \pmod{L}$ が成立し、 $d$ はユークリッドの互除法で算出できる。このとき、 $n$ と $e$ が公開鍵とされ、 $p$ 、 $q$ 、および $d$ が、秘密鍵とされる。

暗号文 $C$ は、平文 $M$ から、式(1)の処理で算出される。

$$C = M^e \pmod{n} \quad \dots\dots (1)$$

暗号文 $C$ は、式(2)の処理で平文 $M$ に、復号される。

$$M = C^d \pmod{n} \quad \dots\dots (2)$$

証明は省略するが、RSA暗号で平文を暗号文に変換して、それが復号できるのは、フェルマーの小定理に根拠をおいており、式(3)が成立するからである。

$$M = C^d = (M^e)^d = M^{ed} = M \pmod{n} \quad \dots\dots (3)$$

秘密鍵 $p$ と $q$ を知っているならば、公開鍵 $e$ から秘密鍵 $d$ は算出できるが、公開鍵 $n$ の素因数分解が計算量的に困難な程度に公開鍵 $n$ の桁数を大きくすれば、公

公開鍵  $n$  を知るだけでは、公開鍵  $e$  から秘密鍵  $d$  は計算できず、復号できない。以上のように、RSA 暗号では、暗号化に使用する鍵と復号するときの鍵を、異なる鍵とすることができる。

また、公開鍵暗号の他の例である楕円曲線暗号 (Elliptic Curve Cryptography) についても、簡単に説明する。楕円曲線  $y^2 = x^3 + ax + b$  上の、ある点を  $B$  とする。楕円曲線上の点の加算を定義し、 $nB$  は、 $B$  を  $n$  回加算した結果を表す。同様に、減算も定義する。 $B$  と  $nB$  から  $n$  を算出することは、困難であることが証明されている。 $B$  と  $nB$  を公開鍵とし、 $n$  を秘密鍵とする。乱数  $r$  を用いて、暗号文  $C1$  および  $C2$  は、平文  $M$  から、公開鍵で式 (4) および式 (5) の処理で算出される。

$$C1 = M + r n B \quad \dots\dots (4)$$

$$C2 = r B \quad \dots\dots (5)$$

暗号文  $C1$  および  $C2$  は、式 (6) の処理で平文  $M$  に、復号される。

$$M = C1 - n C2 \quad \dots\dots (6)$$

復号できるのは、秘密鍵  $n$  を有するものだけである。以上のように、RSA 暗号と同様に、楕円曲線暗号でも、暗号化に使用する鍵と復号するときの鍵を、異なる鍵とすることができる。

図 9 に再び戻り、コンテンツプロバイダ 2 の相互認証部 39 は、EMD サービスセンタ 1 から配送用鍵  $Kd$  の供給を受けるのに先立ち、EMD サービスセンタ 1 と相互認証する。また相互認証部 39 は、サービスプロバイダ 3 へのコンテンツプロバイダセキュアコンテナの送信に先立ち、サービスプロバイダ 3 と相互認証することも可能であるが、この例の場合、コンテンツプロバイダセキュアコン

テナには、秘密にしなければならない情報が含まれていないので、この相互認証は、必ずしも必要とされない。

#### (4) サービスプロバイダ

次に、図15のブロック図を参照して、サービスプロバイダ3の機能的構成を説明する。コンテンツサーバ41は、コンテンツプロバイダ2から供給されたコンテンツプロバイダセキュアコンテナに含まれる、コンテンツ（コンテンツ鍵K<sub>co</sub>で暗号化されている）、コンテンツ鍵K<sub>co</sub>（配送用鍵K<sub>d</sub>で暗号化されている）、UCP、およびコンテンツプロバイダ2の署名を記憶し、セキュアコンテナ作成部44に供給する。

値付け部42は、コンテンツプロバイダ2から供給されたコンテンツプロバイダセキュアコンテナに含まれる署名に基づいて、コンテンツプロバイダセキュアコンテナの正当性を検証し、その正当性を確認すると、コンテンツプロバイダセキュアコンテナに含まれるUCPに対応する、PTを作成し、セキュアコンテナ作成部44に供給する。図16は、図10のUCPAに対応して作成された、2つのPTA-1（図16（A））およびPTA-2（図16（B））を表している。PTには、「コンテンツのID」、「コンテンツプロバイダのID」、「UCPのID」、「サービスプロバイダのID」、「PTのID」、「PTの有効期限」、「価格条件」、および「価格内容」の各項目に設定される所定の情報が含まれる。

PTの、「コンテンツのID」、「コンテンツプロバイダのID」、および「UCPのID」の各項目には、UCPの、これらに対応する項目の情報が、それぞれ設定される。すなわち、PTA-1およびPTA-2のそれぞれの「コンテンツのID」には、コンテンツAのIDが、それぞれの「コンテンツプロバイダのID」には、コンテンツプロバイダ2のIDが、そしてそれぞれの「UCPのID」には、UCPAのIDが設定されている。

「サービスプロバイダのID」には、PTの提供元のサービスプロバイダ3のIDが設定される。PTA-1およびPTA-2のそれぞれの「サービスプロバイダのID」には、サービスプロバイダ3のIDが設定されている。「PTのI

D」には、各PTに割り当てられた所定のIDが設定され、PTA-1の「PTのID」には、PTA-1のIDが、PTA-2の「PTのID」には、PTA-2のIDがそれぞれ設定されている。「PTの有効期限」には、PTの有効期限を示す情報が設定され、PTA-1の「PTの有効期限」には、PTA-1の有効期限が、PTA-2の「PTの有効期限」には、PTA-2の有効期限が設定されている。

「価格条件」は、UCPの「利用条件」と同様に、「ユーザ条件」および「機器条件」の項目からなり、その「ユーザ条件」には、このPTを選択することができるユーザの条件を示す情報が設定され、その「機器条件」には、このPTを選択することができる機器の条件を示す情報が設定される。

PTA-1の場合、「価格条件10」が設定され、「価格条件10」の「ユーザ条件10」には、ユーザが男性であることを示す情報（”男性”）が設定され、その「機器条件10」には、”条件なし”が設定されている。すなわち、PTA-1は、男性のユーザのみが選択可能となる。

PTA-2の場合、「価格条件20」が設定され、「価格条件20」の「ユーザ条件20」には、ユーザが女性であることを示す情報（”女性”）が設定され、その「機器条件20」には、”条件なし”が設定されている。すなわち、PTA-2は、女性のユーザのみが選択可能となる。

PTの「価格内容」には、対応するUCPの「利用内容」の「形式」に設定されている利用形式の利用料金（利用形式でコンテンツを利用する権利の価格）が示されている。PTA-1の「価格内容11」の”2000円”とPTA-2の「価格内容21」の”1000円”は、コンテンツAを”買い取り再生”の利用形式で利用する場合の料金（”買い取り再生”の利用形式で利用する権利の価格）を示している。

PTA-1の「価格内容12」の”600円”およびPTA-2の「価格内容22」の”300円”は、UCPAの「利用内容12」の「形式12」より、”第1世代複製”の利用形式でコンテンツAを利用する権利の価格を示している。

P T A-1の「価格内容13」の”100円”およびP T A-2の「価格内容23」の”50円”は、U C P Aの「利用内容13」の「形式13」より、”期間制限再生”の利用形式でコンテンツAを利用する権利の価格を示している。P T A-1の「価格内容14」の”300円”およびP T A-2の「価格内容24」の”150円”は、U C P Aの「利用内容14」の「形式14」より、”Pay Per Copy N”の利用形式でコンテンツAを利用する権利の価格を示している。

P T A-1の「価格内容15」の”1950円”およびP T A-2の「価格内容25」の”1980円”は、U C P Aの「利用内容15」の「形式15」より、”期間制限再生”の権利を有しているときの、”買い取り再生”の権利の価格を示している。P T A-1の「価格内容16」の”1000円”およびP T A-2の「価格内容26」の”500円”は、U C P Aの「利用内容16」の「形式16」より、”買い取り再生”の権利を有しているときの、”買い取り再生”の権利の価格を示している。

なお、この例の場合、P T A-1（男性ユーザに適用される）の価格内容と、P T A-2（女性ユーザに適用される）の価格内容を比較すると、P T A-1の価格内容に示される価格が、P T A-2の価格内容に示される価格の2倍に設定されている。例えば、U C P Aの「利用内容11」に対応するP T A-1の「価格内容11」が”2000円”とされているのに対し、同様にU C P Aの「利用内容11」に対応するP T A-2の「価格内容21」は”1000円”とされている。同様、P T A-1の「価格内容12」乃至「価格内容14」に設定されている価格は、P T A-2の「価格内容22」乃至「価格内容24」に設定されている価格の2倍とされている。すなわち、コンテンツAは、女性ユーザがより低価格で利用することができるコンテンツである。

図15に戻り、ポリシー記憶部43は、コンテンツプロバイダ2から供給された、コンテンツのU C Pを記憶し、セキュアコンテナ作成部44に供給する。

セキュアコンテナ作成部44は、例えば、図17に示すような、コンテンツA

(コンテンツ鍵  $K_{coA}$  で暗号化されている)、コンテンツ鍵  $K_{coA}$  (配送用鍵  $K_d$  で暗号化されている)、UCPA、コンテンツプロバイダ2の署名、PTA-1, A-2、およびサービスプロバイダ3の署名からなるサービスプロバイダセキュアコンテナを作成する。

セキュアコンテナ作成部44はまた、作成したサービスプロバイダセキュアコンテナを、図18に示すような、証明書のバージョン番号、認証局がサービスプロバイダ3に対し割り付ける証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、サービスプロバイダ3の名前、サービスプロバイダ3の公開鍵  $K_{psp}$ 、並びに認証局の署名より構成されるサービスプロバイダの証明書を付して、ユーザホームネットワーク5に供給する。

図15に、再び戻り、相互認証部45は、コンテンツプロバイダ2からコンテンツプロバイダセキュアコンテナの供給を受け取るのに先立ち、コンテンツプロバイダ2と相互認証する。相互認証部45また、ユーザホームネットワーク5へのサービスプロバイダセキュアコンテナの送信に先立ち、ユーザホームネットワーク5と相互認証するが、このサービスプロバイダ3とユーザホームネットワーク5との相互認証は、例えば、ネットワーク4が衛星通信である場合、実行されない。なお、この例の場合、コンテンツプロバイダセキュアコンテナおよびサービスプロバイダセキュアコンテナには、特に、秘密情報が含まれていないので、サービスプロバイダ3は、コンテンツプロバイダ2およびユーザホームネットワーク5と相互認証を行わなくてもよい。

#### (5) ユーザホームネットワーク

##### (5-1) レシーバ51

図19は、ユーザホームネットワーク5を構成するレシーバ51の構成例を表している。レシーバ51は、通信部61、SAM62、外部記憶部63、伸張部64、通信部65、インタフェース66、表示制御部67、および入力制御部68より構成される据え置き型の機器である。

レシーバ51の通信部61は、ネットワーク4を介してサービスプロバイダ3、またはEMDサービスセンタ1と通信し、所定の情報を受信し、または送信する。

SAM62は、相互認証モジュール71、課金処理モジュール72、記憶モジュール73、復号／暗号化モジュール74、およびデータ検査モジュール75からなるが、シングルチップの暗号処理専用ICで構成され、多層構造を有し、その内部のメモリセルはアルミニウム層等のダミー層に挟まれ、また、動作する電圧または周波数の幅が狭い等、外部から不正にデータが読み出し難い特性（耐タンパー性）を有している。

SAM62の相互認証モジュール71は、記憶モジュール73に記憶されている、図20に示すSAM62の証明書を、相互認証相手に送信し、相互認証を実行し、これにより、認証相手と共有することとなった一時鍵 $K_{temp}$ （セッション鍵）を復号／暗号化モジュール74に供給する。SAMの証明書には、コンテンツプロバイダ2の証明書（図14）およびサービスプロバイダ3の証明書（図18）に含まれている情報に対応する情報が含まれているので、その説明は省略する。

課金処理モジュール72は、選択されたUCPの利用内容に基づいて、使用許諾条件情報UCSおよび課金情報を作成する。図21は、コンテンツが“期限制限再生”の利用形式で権利購入された場合のUCSの例であり、図10に示したUCPAの利用内容13と、図16（A）に示したPTA-1の「価格内容13」に基づいて生成されたUCSAを表している。UCSには、図21に示されるように、「コンテンツのID」、「コンテンツプロバイダのID」、「UCPのID」、「UCPの有効期限」、「サービスプロバイダのID」、「PTのID」、「PTの有効期限」、「UCSのID」、「SAMのID」、「ユーザのID」、「利用内容」、および「利用履歴」の各項目に設定される情報が含まれている。

UCSの、「コンテンツのID」、「コンテンツプロバイダのID」、「UCPのID」、「UCPの有効期限」、「サービスプロバイダのID」、「PTのID」、お

よび「P Tの有効期限」の各項目には、P Tの、それらに対応する項目の情報が設定される。すなわち、図21のUCSAの、「コンテンツのID」には、コンテンツAのIDが、「コンテンツプロバイダのID」には、コンテンツプロバイダ2のIDが、「UCPのID」には、UCPAのIDが、「UCPの有効期限」には、UCPAの有効期限が、「サービスプロバイダのID」には、サービスプロバイダ3のIDが、「P TのID」には、PTA-1のIDが、そして「P Tの有効期限」には、PTA-1の有効期限が、それぞれ設定されている。

「UCSのID」には、UCSに割り当てられた所定のIDが設定され、UCSAの「UCSのID」には、UCSAのIDが設定されている。「SAMのID」には、機器のSAMのIDが設定され、UCSAの「SAMのID」には、レシーバ51のSAM62のIDが設定されている。「ユーザのID」には、コンテンツを利用するユーザのIDが設定され、UCSAの「ユーザのID」には、ユーザFのIDが設定されている。

「利用内容」は、「ID」、「形式」、「パラメータ」、および「管理移動状態情報」の各項目からなり、そのうち「ID」、「形式」、および「パラメータ」の項目には、選択されたUCPの「利用内容」の、それらに対応する項目の情報が設定される。すなわち、UCSAの「ID」には、UCPAの「利用内容13」の「ID13」に設定されている情報（利用内容13のID）が、「形式」には、「利用内容13」の「形式13」に設定されている”期限制限再生”が、「パラメータ」には、「利用内容13」の「パラメータ13」に設定されている情報（開始時期および終了時期）が設定されている。

「利用内容」の「管理移動状態情報」には、選択されたUCPの「管理移動許可情報」に”可”が設定されている場合（管理移動が行える場合）、管理移動元の機器（コンテンツを購入した機器）と管理移動先の機器のそれぞれのIDが設定されるようになされている。なお、コンテンツの管理移動が行われていない状態においては、管理移動元の機器のIDが、管理移動先の機器のIDとしても設定される。UCPの「管理移動許可情報」に、”不可”が設定されている場合、



「管理移動状態情報」には”不可”が設定される。すなわち、この場合、コンテンツの管理移動は行われない（許可されない）。UCSAの「管理移動状態情報」には、UCPAの「利用内容13」の「管理移動許可情報13」に”可”が設定されており、また、このとき、コンテンツAは管理移動されていないので、SAM62のIDが、管理移動元の機器のIDおよび管理移動先の機器のIDとして設定されている。

「利用履歴」には、同一のコンテンツに対する利用形式の履歴が含まれている。UCSAの「利用履歴」には、”期限制限再生”を示す情報のみが記憶されているが、例えば、レシーバ51において、コンテンツAが以前に利用されていた場合、そのときの利用形式を示す情報も記憶されている。

なお、上述したUCSにおいては、「UCPの有効期限」および「PTの有効期限」が、設けられているがそれらをUCSに設定しないようにすることもできる。また、上述したUCSにおいて、「コンテンツプロバイダのID」が設けられているが、UCPのIDがユニークで、これにより、コンテンツプロバイダを特定することができる場合、それを設けないようにすることもできる。また「サービスプロバイダのID」も同様に、PTのIDがユニークで、これにより、サービスプロバイダを特定することができる場合、それを設けないようにすることもできる。

作成されたUCSは、レシーバ51の復号／暗号化モジュール74の復号化ユニット91から供給されるコンテンツ鍵Kco（保存用鍵Ksaveで暗号化されている）とともに、外部記憶部63に送信され、その利用情報記憶部63Aに記憶される。外部記憶部63の利用情報記憶部63Aは、図22に示すように、M個のブロックBP-1乃至BP-Mに分割され（例えば、1メガバイト毎に分割され）、各ブロックBPが、N個の利用情報用メモリ領域RP-1乃至RP-Nに分割されている。SAM62から供給されるコンテンツ鍵Kco（保存用鍵Ksaveで暗号化されている）およびUCSは、利用情報用記憶部63Aの所定のブロックBPの利用情報用メモリ領域RPに、対応して記憶される。

図 2 2 の例では、ブロック B P - 1 の利用情報用メモリ領域 R P - 3 に、図 2 1 に示した U C S A と、コンテンツ鍵 K c o A (保存用鍵 K s a v e で暗号化されている) が対応して記憶されている。ブロック B P - 1 の利用情報用メモリ領域 R P - 1, R P - 2 には、他のコンテンツ鍵 K c o 1, K c o 2 (それぞれ保存用鍵 K s a v e で暗号化されている) および U C S 1, 2 がそれぞれ記憶されている。ブロック B P - 1 の利用情報用メモリ領域 R P - 4 (図示せず) 乃至 R P - N、およびブロック B P - 2 (図示せず) 乃至 B P - M には、この場合、コンテンツ鍵 K c o および U C S は記憶されておらず、空いていることを示す所定の初期情報が記憶されている。なお、利用情報用メモリ領域 R P に記憶されるコンテンツ鍵 K c o (保存用鍵 K s a v e で暗号化されている) および U C S を、個々に区別する必要がない場合、まとめて、利用情報と称する。

図 2 3 は、図 2 1 に示した U C S A と同時に作成された課金情報 A を表している。課金情報には、図 2 3 に示されるように、「コンテンツの I D」、「コンテンツプロバイダの I D」、「U C P の I D」、「U C P の有効期限」、「サービスプロバイダの I D」、「P T の I D」、「P T の有効期限」、「U C S の I D」、「S A M の I D」、「ユーザの I D」、および「利用内容」の各項目に設定される所定の情報が含まれる。

課金情報の、「コンテンツの I D」、「コンテンツプロバイダの I D」、「U C P の I D」、「U C P の有効期限」、「サービスプロバイダの I D」、「P T の I D」、「P T の有効期限」、「U C S の I D」、「S A M の I D」、「ユーザの I D」、および「利用内容」には、U C S の、それらに対応する項目の情報が、それぞれ設定される。すなわち、図 2 3 の課金情報 A の、「コンテンツの I D」には、コンテンツ A の I D が、「コンテンツプロバイダの I D」には、コンテンツプロバイダ 2 の I D が、「U C P の I D」には、U C P A の I D が、「U C P の有効期限」には、U C P A の有効期限が、「サービスプロバイダの I D」には、サービスプロバイダ 3 の I D が、「P T の I D」には、P T A - 1 の I D が、「P T の有効期限」には、P T A - 1 の有効期限が、「U C S の I D」には、U C S A の I D が

、「SAMのID」には、SAM62のIDが、「ユーザのID」には、レシーバ51のユーザFのIDが、そして「利用内容」には、UCSAの「利用内容13」の内容が、それぞれ設定されている。

なお、上述した課金情報においては、「UCPの有効期限」および「PTの有効期限」が、設けられているがそれらをUCSに設定しないようにすることもできる。また、上述した課金情報において、「コンテンツプロバイダのID」が設けられているが、UCPのIDがユニークで、これにより、コンテンツプロバイダを特定することができる場合、それを設けないようにすることもできる。また「サービスプロバイダのID」も同様に、PTのIDがユニークで、これにより、サービスプロバイダを特定することができる場合、それを設けないようにすることもできる。

図19に戻り、記憶モジュール73には、図24に示すように、SAM62の公開鍵Kpu、SAM62の秘密鍵Ksu、EMDサービスセンタ1の公開鍵Kpesc、認証局の公開鍵Kpca、保存用鍵Ksave、3ヶ月分の配送用鍵Kdなどの各種鍵、SAM62の証明書、課金情報（例えば、図23の課金情報A）、基準情報51、およびM個の検査値HP-1乃至HP-Mなどが記憶されている。

記憶モジュール73に記憶される検査値HP-1は、外部記憶部63の利用情報記憶部63A（図22）のブロックBP-1に記憶されているデータの全体にハッシュ関数が適用されて算出されたハッシュ値である。検査値HP-2乃至HP-Mも、検査値HP-1と同様に、外部記憶部63の、対応するブロックBP-2乃至BP-Mのそれぞれに記憶されているデータにハッシュ関数が適用されて算出されたハッシュ値である。

図25は、記憶モジュール73に記憶されている基準情報51を表している。基準情報には、「SAMのID」、「機器番号」、「決済ID」、「課金の上限額」、「決済ユーザ情報」、「従属ユーザ情報」、および「利用ポイント情報」の各項目に設定される所定の情報が含まれる。

基準情報の、「SAMのID」、「機器番号」、「決済ID」、「決済ユーザ情報」、「従属ユーザ情報」、および「利用ポイント情報」には、EMDサービスセンタ1のユーザ管理部18により管理されているシステム登録情報の、SAM62のIDに対応する項目の情報が設定される。すなわち、基準情報51には、SAM62のID、SAM62の機器番号(100番)、ユーザFの決済ID、ユーザFの決済ユーザ情報(ユーザFの一般情報(氏名、住所、電話番号、決済機関情報、生年月日、年齢、性別)、ユーザFのID、およびユーザFのパスワード)、およびレシーバ51の利用ポイント情報が設定されている。

「課金の上限額」には、機器がEMDシステム正式登録されている状態と仮登録されている状態で、それぞれ異なる額を示す、課金の上限額が設定されている。

基準情報51の「課金の上限額」には、レシーバ51が正式登録されているので、正式登録されている状態における課金の上限額を示す情報(“正式登録時の上限額”)が設定されている。

図19に戻り、SAM62の復号/暗号化モジュール74は、復号ユニット91、乱数発生ユニット92、および暗号化ユニット93から構成される。復号ユニット91は、暗号化されたコンテンツ鍵Kcoを配送用鍵Kdで復号し、暗号化ユニット93に出力する。乱数発生ユニット92は、相互認証時に、所定の桁数の乱数を発生し、必要に応じて一時鍵Ktempを生成し、暗号化ユニット93に出力する。

暗号化ユニット93は、復号されたコンテンツ鍵Kcoを、再度、記憶モジュール73に保持されている保存用鍵Ksaveで暗号化する。暗号化されたコンテンツ鍵Kcoは、外部記憶部63に供給される。暗号化ユニット93は、コンテンツ鍵Kcoを伸張部64に送信するとき、コンテンツ鍵Kcoを乱数発生ユニット92で生成した一時鍵Ktempで暗号化する。

データ検査モジュール75は、記憶モジュール73に記憶されている検査値HPと、外部記憶部63の利用情報記憶部63Aの、対応するブロックBPのデー

タのハッシュ値を比較し、ブロックBPのデータが改竄されていないか否かを検査する。

伸張部64は、相互認証モジュール101、復号モジュール102、復号モジュール103、伸張モジュール104、およびウォーターマーク付加モジュール105から構成される。相互認証モジュール101は、SAM62と相互認証し、一時鍵Ktempを復号モジュール102に出力する。復号モジュール102は、一時鍵Ktempで暗号化されたコンテンツ鍵Kcoを一時鍵Ktempで復号し、復号モジュール103に出力する。復号モジュール103は、HDD52に記録されたコンテンツをコンテンツ鍵Kcoで復号し、伸張モジュール104に出力する。伸張モジュール104は、復号されたコンテンツを、更にATTRAC2等の方式で伸張し、ウォーターマーク付加モジュール105に出力する。ウォーターマーク付加モジュール105は、コンテンツにレシーバ51を特定する所定のウォーターマーク（電子透かし）を挿入し、図示せぬスピーカに出力し、音楽を再生する。

通信部65は、ユーザホームネットワーク5のレシーバ201およびレシーバ301との通信処理を行う。インターフェース66は、SAM62および伸張部64からの信号を所定の形式に変更し、HDD52に出力し、また、HDD52からの信号を所定の形式に変更し、SAM62および伸張部64に出力する。

表示制御部67は、表示部（図示せず）への出力を制御する。入力制御部68は、各種ボタンなどから構成される操作部（図示せず）からの入力を制御する。

HDD52は、サービスプロバイダ3から供給されたコンテンツなどを記憶する他、図26に示すような登録リストを記憶している。この登録リストは、表形式に情報が記憶されているリスト部、および登録リストを保持する機器についての所定の情報が記憶されている対象SAM情報部より構成されている。

対象SAM情報部には、この登録リストを保有する機器のSAMID、この例の場合、レシーバ51のSAM62のIDが（「対象SAMID」の欄に）記憶されている。対象SAM情報部にはまた、この登録リストの有効期限が（「有効

期限」の欄に) 記憶され、登録リストのバージョン番号が(「バージョン番号」の欄に) 記憶され、そして接続されている機器の数(自分自身を含む)、この例の場合、レシーバ51には、レシーバ201およびレシーバ301の2機の機器が接続されているので、自分自身を含む合計値3が(「接続されている機器数」の欄に) 記憶されている。

リスト部は、「SAM ID」、「ユーザID」、「購入処理」、「課金処理」、「課金機器」、「コンテンツ供給機器」、「状態フラグ」、「登録条件署名」、および「登録リスト署名」の9個の項目から構成され、この例の場合、レシーバ51の登録条件、レシーバ201の登録条件、およびレシーバ301の登録条件が記憶されている。

「SAM ID」には、機器のSAMのIDが記憶される。この例の場合、レシーバ51のSAM62のID、レシーバ201のSAM212のID、およびレシーバ301のSAM311のIDが記憶されている。「ユーザID」には、決済ユーザのIDが記憶される。この例の場合、ユーザFのIDが、レシーバ51、レシーバ201、およびレシーバ301に対応する「ユーザID」に、それぞれ記憶されている。

「購入処理」には、機器が、コンテンツを購入するための処理を行うことができるか否かを示す情報(“可”または“不可”)が記憶される。この例の場合、レシーバ51およびレシーバ201は、コンテンツを購入するための処理を行うことができるようになされているので、それらに対応する「購入処理」には、“可”が記憶されている。レシーバ301は、購入処理を行うことができないものとされているので、対応する「購入処理」には、“不可”が記憶されている。

「課金処理」には、機器が、EMDサービスセンタ1との間で、課金処理を行うことができるか否かを示す情報(“可”または“不可”)が記憶される。この例の場合、レシーバ51およびレシーバ201は、課金処理を行うことができるようになされているので、それらに対応する「課金処理」には、それぞれ“可”が記憶される。レシーバ301は、課金処理を行うことができないものとされてい

るので、対応する「課金処理」には、“不可”が記憶されている。

「課金機器」には、計上された課金を決済する処理を行う機器のSAMのIDが記憶される。この例の場合、レシーバ51およびレシーバ201は、自分自身で課金処理を行うことができるので、それらに対応する「課金機器」には、自分自身のSAMのIDが記憶されている。レシーバ301は、コンテンツの購入および課金も行われないので、対応する「課金機器」には、“なし”が記憶されている。

「コンテンツ供給機器」には、機器が、コンテンツの供給をサービスプロバイダ3からではなく、接続される他の機器から受ける場合、コンテンツを供給することができる機器のSAMのIDが記憶される。この例の場合、レシーバ51は、コンテンツの供給をサービスプロバイダ3から受けるので、「コンテンツ供給機器」には、コンテンツを供給する機器が存在しないことを示す情報（“なし”）が記憶されている。レシーバ201およびレシーバ301は、コンテンツの供給をレシーバ51から受けるので、対応する「コンテンツ供給機器」には、レシーバ51のSAM62のIDが設定されている。

「状態フラグ」には、機器の動作制限条件が記憶される。何ら制限されていない場合は、その旨を示す情報（“制限なし”）、一定の制限が課せられている場合は、その旨を示す情報（“制限あり”）、また動作が停止させられている場合には、その旨を示す情報（“停止”）が記憶される。例えば、課金の決済が成功しなかった場合、その機器に対応する「状態フラグ」には、“制限あり”が設定される。この例の場合、「状態フラグ」に“制限あり”が設定された機器においては、すでに購入されたコンテンツを利用するための処理は実行されるが、新たなコンテンツを購入するための処理は実行されなくなる。すなわち、一定の制限が機器に課せられる。また、コンテンツの不正複製などの違反行為が発覚した場合、「状態フラグ」には、“停止”が設定され、機器の動作が停止される。これにより、その機器はEMDシステムからのサービスを、一切受けることができなくなる。

この例の場合、レシーバ51、レシーバ201、およびレシーバ301に対しては、何ら制限が課せられていないものとし、それぞれに対応する「状態フラグ」には、“なし”が設定されている。なお、「状態フラグ」に設定される、“制限あり”および“停止”など、これにより動作が制限される情報を、個々に区別する必要がない場合、まとめて、動作制限情報と称する。

「登録条件署名」には、上述したように、各登録条件として、それぞれ、「SAMID」、「ユーザID」、「購入処理」、「課金処理」、「課金機器」、「コンテンツ供給機器」、および「状態フラグ」に記憶されている情報に対するEMDサービスセンタ1による署名が記憶されている。「登録リスト署名」には、登録リストに設定されているデータの全体に対する署名が記憶されている。

#### (5-2) レシーバ201

図27は、レシーバ201の構成例を表している。レシーバ201の通信部211乃至入力制御部218は、レシーバ51の通信部61乃至入力制御部68と同様の機能を有しているので、その詳細な説明は適宜省略するが、レシーバ201の記憶モジュール223には、図28に示すような基準情報201が記憶されている。基準情報201には、EMDサービスセンタ1のユーザ管理部18により管理されているシステム登録情報の、SAM212のIDに対応して記憶されている、SAM212のID、レシーバ201の機器番号(100番)、ユーザFの決済ID、ユーザFの決済ユーザ情報(ユーザFの一般情報(氏名、住所、電話番号、決済機関情報、生年月日、年齢、性別)、ユーザFのID、およびユーザFのパスワード)、ユーザAの従属ユーザ情報(ユーザAの一般情報(氏名、住所、電話番号、生年月日、性別)、ユーザAのID、およびユーザAのパスワード)、およびレシーバ201の利用ポイント情報が設定されている。「課金の上限額」には、“正式登録時の上限額”が設定されている。

HDD202も、HDD51に記憶されている情報が記憶されているので、その説明は省略するが、図29に示すようなレシーバ201の登録リストが記憶されている。この登録リストの対象SAM情報部には、レシーバ201のSAM2



12のID、その登録リストの有効期限、バージョン番号、接続されている機器の数（この例では、レシーバ201には、レシーバ51の1機が接続されているので、自分自身を含めた合計数2）が記憶されている。リスト部には、図26のレシーバ51の登録リストの、レシーバ51およびレシーバ201の登録条件が記憶されている。

#### （5-3）レシーバ301

図30は、レシーバ301の機能的構成例を表している。レシーバ301は、レシーバ201のSAM212乃至通信部215と基本的に同様の機能を有する、SAM311乃至通信部314を有しているが、レシーバ201の、通信部211、インタフェース216、表示制御部217、および入力制御部218に対応する機能を有しない、携帯型の機器である。

図31は、レシーバ301の記憶モジュール323に記憶されている基準情報301を表している。基準情報301には、EMDサービスセンタ1のユーザ管理部18により管理されているシステム登録情報の、SAM311のIDに対応して記憶されている、SAM311のID、SAM311の機器番号（25番）、ユーザFの決済ID、ユーザFの決済ユーザ情報（ユーザFの一般情報（氏名、住所、電話番号、決済機関情報、生年月日、年齢、性別）、ユーザFのID、およびユーザFのパスワード）、ユーザAの従属ユーザ情報（ユーザAの一般情報（氏名、住所、電話番号、生年月日、性別）、ユーザAのID、およびユーザAのパスワード）、およびレシーバ301の利用ポイント情報が設定されている。「課金の上限額」には、レシーバ301が正式登録されているので、正式登録されている状態における課金の上限額を示す情報（”正式登録時の上限額”）が設定されている。

図32に示すようなレシーバ301の登録リストは、記憶モジュール323に記憶されている。この登録リストの対象SAM情報部には、この登録リストを保有するレシーバ301のSAM311のIDが（「対象SAMID」の欄に）記憶され、その登録リストの有効期限が（「有効期限」の欄に）記憶され、登録リ

ストのバージョン番号が（「バージョン番号」の欄に）記憶され、そして接続されている機器の数（自分自身を含む）、この例の場合、レシーバ301には、レシーバ51の1機の機器が接続されているので、自分自身を含む合計数2が（「接続されている機器数」の欄に）記憶されている。リスト部には、図26のレシーバ51の登録リストの、レシーバ301の登録条件が記憶されているが、この場合、「登録条件署名」および「登録リスト署名」は、削除されている。これは、登録リストの署名の確認後、取り除かれたためで、これにより、記憶モジュール323の記憶容量を節約することができる。なお、この例の場合、1つの署名あたり、40バイトが必要とされる。

#### （6）コンテンツの購入及び利用

次に、EMDシステムの処理について、図33のフローチャートを参照して説明するが、なお、ここでは、ユーザFが、レシーバ51を介して、コンテンツAを購入し、利用する場合を例として説明する。

（6-1）EMDサービスセンタからコンテンツプロバイダへの配送用鍵の伝送  
ステップS11において、配送用鍵Kdが、EMDサービスセンタ1からコンテンツプロバイダ2に供給されるが、この処理の詳細は、図34のフローチャートに示されている。すなわち、ステップS31において、EMDサービスセンタ1の相互認証部17は、コンテンツプロバイダ2の相互認証部39と相互認証し、コンテンツプロバイダ2が、正当なプロバイダであることが確認された後、EMDサービスセンタ1のコンテンツプロバイダ管理部12は、鍵サーバ14から供給された配送用鍵Kdをコンテンツプロバイダ2に送信する。なお、相互認証処理の詳細は、図35乃至図37を参照して後述する。

次に、ステップS32において、コンテンツプロバイダ2の暗号化部36は、EMDサービスセンタ1から送信された配送用鍵Kdを受信し、ステップS33において、記憶する。

このように、コンテンツプロバイダ2の暗号化部36が、配送用鍵Kdを記憶したとき、処理は終了し、図33のステップS12に進む。ここで、ステップS

12の処理の説明の前に、図34のステップS31における相互認証処理（なりすましが無いことを確認する処理）について、1つの共通鍵を用いる場合（図35）、2つの共通鍵を用いる場合（図36）、および公開鍵暗号を用いる場合（図37）を例として説明する。

図35は、1つの共通鍵で、共通鍵暗号であるDESを用いる、コンテンツプロバイダ2の相互認証部39とEMDサービスセンタ1の相互認証部17との相互認証の動作を説明するフローチャートである。ステップS41において、コンテンツプロバイダ2の相互認証部39は、64ビットの乱数R1を生成する（乱数生成部35が生成するようにしてもよい）。ステップS42において、コンテンツプロバイダ2の相互認証部39は、DESを用いて乱数R1を、予め記憶している共通鍵Kcで暗号化する（暗号化部36で暗号化するようにしてもよい）。ステップS43において、コンテンツプロバイダ2の相互認証部39は、暗号化された乱数R1をEMDサービスセンタ1の相互認証部17に送信する。

ステップS44において、EMDサービスセンタ1の相互認証部17は、受信した乱数R1を予め記憶している共通鍵Kcで復号する。ステップS45において、EMDサービスセンタ1の相互認証部17は、32ビットの乱数R2を生成する。ステップS46において、EMDサービスセンタ1の相互認証部17は、復号した64ビットの乱数R1の下位32ビットを乱数R2で入れ替え、接続 $R_{1_H} \parallel R_2$ を生成する。なお、ここで $R_{1_H}$ は、R1の上位nビットを表し、 $A \parallel B$ は、AとBの接続（nビットのAの下位に、mビットのBを結合して、(n+m)ビットとしたもの）を表す。ステップS47において、EMDサービスセンタ1の相互認証部17は、DESを用いて $R_{1_H} \parallel R_2$ を共通鍵Kcで暗号化する。ステップS48において、EMDサービスセンタ1の相互認証部17は、暗号化した $R_{1_H} \parallel R_2$ をコンテンツプロバイダ2に送信する。

ステップS49において、コンテンツプロバイダ2の相互認証部39は、受信した $R_{1_H} \parallel R_2$ を共通鍵Kcで復号する。ステップS50において、コンテンツプロバイダ2の相互認証部39は、復号した $R_{1_H} \parallel R_2$ の上位32ビットR

1 Hを調べ、ステップS 4 1で生成した、乱数R 1の上位3 2ビットR 1<sub>H</sub>と一致すれば、EMDサービスセンタ1が正当なセンタであることを認証する。生成した乱数R 1<sub>H</sub>と、受信したR 1<sub>H</sub>が一致しないとき、処理は終了される。両者が一致するとき、ステップS 5 1において、コンテンツプロバイダ2の相互認証部3 9は、3 2ビットの乱数R 3を生成する。ステップS 5 2において、コンテンツプロバイダ2の相互認証部3 9は、受信して復号したR 1<sub>H</sub> || R 2から下位3 2ビットを取り出した乱数R 2を上位に設定し、生成した乱数R 3をその下位に設定し、接続R 2 || R 3とする。ステップS 5 3において、コンテンツプロバイダ2の相互認証部3 9は、DESを用いて接続R 2 || R 3を共通鍵K<sub>c</sub>で暗号化する。ステップS 5 4において、コンテンツプロバイダ2の相互認証部3 9は、暗号化された接続R 2 || R 3をEMDサービスセンタ1の相互認証部1 7に送信する。

ステップS 5 5において、EMDサービスセンタ1の相互認証部1 7は、受信した接続R 2 || R 3を共通鍵K<sub>c</sub>で復号する。ステップS 5 6において、EMDサービスセンタ1の相互認証部1 7は、復号した接続R 2 || R 3の上位3 2ビットを調べ、乱数R 2と一致すれば、コンテンツプロバイダ2を正当なプロバイダとして認証し、一致しなければ、不正なプロバイダとして、処理を終了する。

図3 6は、2つの共通鍵K<sub>c</sub>1, K<sub>c</sub>2で、共通鍵暗号であるDESを用いる、コンテンツプロバイダ2の相互認証部3 9とEMDサービスセンタ1の相互認証部1 7との相互認証の動作を説明するフローチャートである。ステップS 6 1において、コンテンツプロバイダ2の相互認証部3 9は、6 4ビットの乱数R 1を生成する。ステップS 6 2において、コンテンツプロバイダ2の相互認証部3 9は、DESを用いて乱数R 1を予め記憶している共通鍵K<sub>c</sub>1で暗号化する。ステップS 6 3において、コンテンツプロバイダ2の相互認証部3 9は、暗号化された乱数R 1をEMDサービスセンタ1に送信する。

ステップS 6 4において、EMDサービスセンタ1の相互認証部1 7は、受信した乱数R 1を予め記憶している共通鍵K<sub>c</sub>1で復号する。ステップS 6 5にお

いて、EMDサービスセンタ1の相互認証部17は、乱数R1を予め記憶している共通鍵Kc2で暗号化する。ステップS66において、EMDサービスセンタ1の相互認証部17は、64ビットの乱数R2を生成する。ステップS67において、EMDサービスセンタ1の相互認証部17は、乱数R2を共通鍵Kc2で暗号化する。ステップS68において、EMDサービスセンタ1の相互認証部17は、暗号化された乱数R1および乱数R2をコンテンツプロバイダ2の相互認証部39に送信する。

ステップS69において、コンテンツプロバイダ2の相互認証部39は、受信した乱数R1および乱数R2を予め記憶している共通鍵Kc2で復号する。ステップS70において、コンテンツプロバイダ2の相互認証部39は、復号した乱数R1を調べ、ステップS61で生成した乱数R1（暗号化する前の乱数R1）と一致すれば、EMDサービスセンタ1を適正なセンタとして認証し、一致しなければ、不正なセンタであるとして、処理を終了する。ステップS71において、コンテンツプロバイダ2の相互認証部39は、復号して得た乱数R2を共通鍵Kc1で暗号化する。ステップS72において、コンテンツプロバイダ2の相互認証部39は、暗号化された乱数R2をEMDサービスセンタ1に送信する。

ステップS73において、EMDサービスセンタ1の相互認証部17は、受信した乱数R2を共通鍵Kc1で復号する。ステップS74において、EMDサービスセンタ1の相互認証部17は、復号した乱数R2が、ステップS66で生成した乱数R2（暗号化する前の乱数R2）と一致すれば、コンテンツプロバイダ2を適正なプロバイダとして認証し、一致しなければ、不正なプロバイダであるとして処理を終了する。

図37は、公開鍵暗号である、160ビット長の楕円曲線暗号を用いる、コンテンツプロバイダ2の相互認証部39とEMDサービスセンタ1の相互認証部17との相互認証の動作を説明するフローチャートである。ステップS81において、コンテンツプロバイダ2の相互認証部39は、64ビットの乱数R1を生成する。ステップS82において、コンテンツプロバイダ2の相互認証部39は、

自分自身の公開鍵 $K_{pcp}$ を含む証明書（認証局から予め取得しておいたもの）と、乱数 $R_1$ をEMDサービスセンタ1の相互認証部17に送信する。

ステップS83において、EMDサービスセンタ1の相互認証部17は、受信した証明書の署名（認証局の秘密鍵 $K_{sca}$ で暗号化されている）を、予め取得しておいた認証局の公開鍵 $K_{pca}$ で復号し、コンテンツプロバイダ2の公開鍵 $K_{pcp}$ とコンテンツプロバイダ2の名前のハッシュ値を取り出すとともに、証明書に平文のまま格納されているコンテンツプロバイダ2の公開鍵 $K_{pcp}$ およびコンテンツプロバイダ2の名前を取り出す。証明書が認証局が発行した適正なものであれば、証明書の署名を復号することが可能であり、復号して得られた公開鍵 $K_{pcp}$ およびコンテンツプロバイダ2の名前のハッシュ値は、平文のまま証明書に格納されていたコンテンツプロバイダ2の公開鍵 $K_{pcp}$ およびコンテンツプロバイダ2の名前にハッシュ関数を適用して得られたハッシュ値と一致する。これにより、公開鍵 $K_{pcp}$ が改竄されたものでない適正なものであることが認証される。署名を復号出来なかったり、できたとしてもハッシュ値が一致しないときには、適正な公開鍵でないか、適正なプロバイダでないことになる。この時処理は終了される。

適正な認証結果が得られたとき、ステップS84において、EMDサービスセンタ1の相互認証部17は、64ビットの乱数 $R_2$ を生成する。ステップS85において、EMDサービスセンタ1の相互認証部17は、乱数 $R_1$ および乱数 $R_2$ の接続 $R_1 \parallel R_2$ を生成する。ステップS86において、EMDサービスセンタ1の相互認証部17は、接続 $R_1 \parallel R_2$ を自分自身の秘密鍵 $K_{sesc}$ で暗号化する。ステップS87において、EMDサービスセンタ1の相互認証部17は、接続 $R_1 \parallel R_2$ を、ステップS83で取得したコンテンツプロバイダ2の公開鍵 $K_{pcp}$ で暗号化する。ステップS88において、EMDサービスセンタ1の相互認証部17は、秘密鍵 $K_{sesc}$ で暗号化された接続 $R_1 \parallel R_2$ 、公開鍵 $K_{pcp}$ で暗号化された接続 $R_1 \parallel R_2$ 、および自分自身の公開鍵 $K_{pesc}$ を含む証明書（認証局から予め取得しておいたもの）をコンテンツプロバイダ2の相

互認証部 39 に送信する。

ステップ S 89 において、コンテンツプロバイダ 2 の相互認証部 39 は、受信した証明書の署名を予め取得しておいた認証局の公開鍵  $K_{pca}$  で復号し、正しければ証明書から公開鍵  $K_{pesc}$  を取り出す。この場合の処理は、ステップ S 83 における場合と同様であるので、その説明は省略する。ステップ S 90 において、コンテンツプロバイダ 2 の相互認証部 39 は、EMD サービスセンタ 1 の秘密鍵  $K_{sec}$  で暗号化されている接続  $R_1 \parallel R_2$  を、ステップ S 89 で取得した公開鍵  $K_{pesc}$  で復号する。ステップ S 91 において、コンテンツプロバイダ 2 の相互認証部 39 は、自分自身の公開鍵  $K_{pcp}$  で暗号化されている接続  $R_1 \parallel R_2$  を、自分自身の秘密鍵  $K_{scp}$  で復号する。ステップ S 92 において、コンテンツプロバイダ 2 の相互認証部 39 は、ステップ S 90 で復号された接続  $R_1 \parallel R_2$  と、ステップ S 91 で復号された接続  $R_1 \parallel R_2$  を比較し、一致すれば EMD サービスセンタ 1 を適正なものとして認証し、一致しなければ、不適正なものとして、処理を終了する。

適正な認証結果が得られたとき、ステップ S 93 において、コンテンツプロバイダ 2 の相互認証部 39 は、64 ビットの乱数  $R_3$  を生成する。ステップ S 94 において、コンテンツプロバイダ 2 の相互認証部 39 は、ステップ S 90 で取得した乱数  $R_2$  および生成した乱数  $R_3$  の接続  $R_2 \parallel R_3$  を生成する。ステップ S 95 において、コンテンツプロバイダ 2 の相互認証部 39 は、接続  $R_2 \parallel R_3$  を、ステップ S 89 で取得した公開鍵  $K_{pesc}$  で暗号化する。ステップ S 96 において、コンテンツプロバイダ 2 の相互認証部 39 は、暗号化した接続  $R_2 \parallel R_3$  を EMD サービスセンタ 1 の相互認証部 17 に送信する。

ステップ S 97 において、EMD サービスセンタ 1 の相互認証部 17 は、暗号化された接続  $R_2 \parallel R_3$  を自分自身の秘密鍵  $K_{sec}$  で復号する。ステップ S 98 において、EMD サービスセンタ 1 の相互認証部 17 は、復号した乱数  $R_2$  が、ステップ S 84 で生成した乱数  $R_2$ （暗号化する前の乱数  $R_2$ ）と一致すれば、コンテンツプロバイダ 2 を適正なプロバイダとして認証し、一致しなければ、

不適正なプロバイダとして、処理を終了する。

以上のように、E M Dサービスセンタ 1 の相互認証部 1 7 とコンテンツプロバイダ 2 の相互認証部 3 9 は、相互認証する。相互認証に利用された乱数は、その相互認証に続く処理にだけ有効な一時鍵  $K_{temp}$  として利用される。

(6-2) コンテンツプロバイダからサービスプロバイダへのコンテンツの伝送  
次に、図 3 3 のステップ S 1 2 の処理について説明する。ステップ S 1 2 においては、コンテンツプロバイダセキュアコンテナが、コンテンツプロバイダ 2 からサービスプロバイダ 3 に供給される。その処理の詳細は、図 3 8 のフローチャートに示されている。すなわち、ステップ S 2 0 1 において、コンテンツプロバイダ 2 のウォータマーク付加部 3 2 (図 9) は、コンテンツサーバ 3 1 からコンテンツ A を読み出し、コンテンツプロバイダ 2 を示す所定のウォータマーク (電子透かし) を挿入し、圧縮部 3 3 に供給する。

ステップ S 2 0 2 において、コンテンツプロバイダ 2 の圧縮部 3 3 は、ウォータマークが挿入されたコンテンツ A を A T R A C 2 等の所定の方式で圧縮し、暗号化部 3 4 に供給する。ステップ S 2 0 3 において、乱数発生部 3 5 は、コンテンツ鍵  $K_{coA}$  となる乱数を発生させ、暗号化部 3 4 に供給する。

ステップ S 2 0 4 において、コンテンツプロバイダ 2 の暗号化部 3 4 は、D E S などの所定の方式で、乱数発生部 3 5 で発生された乱数 (コンテンツ鍵  $K_{coA}$ ) を使用して、ウォータマークが挿入されて圧縮されたコンテンツ A を暗号化する。次に、ステップ S 2 0 5 において、暗号化部 3 6 は、D E S などの所定の方式で、E M D サービスセンタ 1 から供給された配送用鍵  $K_d$  でコンテンツ鍵  $K_{coA}$  を暗号化する。

ステップ S 2 0 6 において、コンテンツプロバイダ 2 のセキュアコンテナ作成部 3 8 は、コンテンツ A (コンテンツ鍵  $K_{coA}$  で暗号化されている)、コンテンツ鍵  $K_{coA}$  (配送用鍵  $K_d$  で暗号化されている)、およびコンテンツ A に対応する U C P A の全体にハッシュ関数を適用してハッシュ値を算出し、自分自身の秘密鍵  $K_{scp}$  で暗号化する。これにより、図 1 3 に示した署名が作成される



ステップS 2 0 7において、コンテンツプロバイダ2のセキュアコンテナ作成部3 8は、コンテンツA（コンテンツ鍵K c o Aで暗号化されている）、コンテンツ鍵K c o A（配送用鍵K dで暗号化されている）、UCPA、およびステップS 2 0 6で生成した署名を含んだ、図1 3に示したコンテンツプロバイダセキュアコンテナを作成する。

ステップS 2 0 8において、コンテンツプロバイダ2の相互認証部3 9は、サービスプロバイダ3の相互認証部4 5と相互認証する。この認証処理は、図3 5乃至図3 7を参照して説明した場合と同様であるので、その説明は省略する。ステップS 2 0 9において、コンテンツプロバイダ2のセキュアコンテナ作成部3 8は、認証局から予め発行された証明書を、ステップS 2 0 7で作成したコンテンツプロバイダセキュアコンテナに付して、サービスプロバイダ3に送信する。

このようにして、コンテンツプロバイダセキュアコンテナが、サービスプロバイダ3に供給されたとき、処理は終了し、図3 3のステップS 1 3に進む。

#### （6－3）サービスプロバイダからレシーバへのコンテンツの伝送

ステップS 1 3において、サービスプロバイダセキュアコンテナが、サービスプロバイダ3からユーザホームネットワーク5（レシーバ5 1）に供給される。この処理の詳細は、図3 9のフローチャートに示されている。すなわち、ステップS 2 2 1において、サービスプロバイダ3の値付け部4 2は、コンテンツプロバイダ2から送信されたコンテンツプロバイダセキュアコンテナに付された証明書に含まれる署名を確認し、証明書の改竄がなければ、それから、コンテンツプロバイダ2の公開鍵K p c pを取り出す。証明書の署名の確認は、図3 7のステップS 8 3における処理と同様であるので、その説明は省略する。

ステップS 2 2 2において、サービスプロバイダ3の値付け部4 2は、コンテンツプロバイダ2から送信されたコンテンツプロバイダセキュアコンテナの署名をコンテンツプロバイダ2の公開鍵K p c pで復号し、得られたハッシュ値が、コンテンツA（コンテンツ鍵K c o Aで暗号化されている）、コンテンツ鍵K c

○ A（配送用鍵 K d で暗号化されている）、および U C P A の全体にハッシュ関数を適用して得られたハッシュ値と一致するか否かを判定し、コンテンツプロバイダセキュアコンテナの改竄がないことを確認する。両者の値が一致しない場合（改竄が発見された場合）は、処理は終了されるが、この例の場合、コンテンツプロバイダセキュアコンテナの改竄はなかったものとし、ステップ S 2 2 3 に進む。

ステップ S 2 2 3 において、サービスプロバイダ 3 の値付け部 4 2 は、コンテンツプロバイダセキュアコンテナから、コンテンツ A（コンテンツ鍵 K c o A で暗号化されている）、コンテンツ鍵 K c o A（配送用鍵 K d で暗号化されている）、およびコンテンツプロバイダ 2 の署名を取り出し、コンテンツサーバ 4 1 に供給する。コンテンツサーバ 4 1 は、それらを記憶する。値付け部 4 2 はまた U C P A も、コンテンツプロバイダセキュアコンテナから取り出し、セキュアコンテナ作成部 4 4 に供給する。

ステップ S 2 2 4 において、サービスプロバイダ 3 の値付け部 4 2 は、取り出した U C P A に基づいて、P T A - 1, A - 2 を作成し、セキュアコンテナ作成部 4 4 に供給する。

ステップ S 2 2 5 において、サービスプロバイダ 3 のセキュアコンテナ作成部 4 4 は、コンテンツ A（コンテンツ鍵 K c o A で暗号化されている）、コンテンツ鍵 K c o A（配送用鍵 K d で暗号化されている）、コンテンツプロバイダ 2 の署名、U C P A、P T A - 1, A - 2、およびサービスプロバイダ 3 の署名から、図 1 7 に示したサービスプロバイダセキュアコンテナを作成する。

ステップ S 2 2 6 において、サービスプロバイダ 3 の相互認証部 4 5 は、レシーバ 5 1 の相互認証モジュール 7 1 と相互認証する。この認証処理は、図 3 5 乃至図 3 7 を参照して説明した場合と同様であるので、その説明を省略する。

ステップ S 2 2 7 において、サービスプロバイダ 3 のセキュアコンテナ作成部 4 4 は、ステップ S 2 2 5 で作成したサービスプロバイダセキュアコンテナに、サービスプロバイダ 3 の証明書を付して、ユーザホームネットワーク 5 のレシー

バ51に送信する。

このようにして、サービスプロバイダセキュアコンテナが、サービスプロバイダ3からレシーバ51に送信されたとき、処理は終了し、図33のステップS14に進む。

#### (6-4) レシーバによるコンテンツの記録処理

ステップS14において、サービスプロバイダ3から送信されたサービスプロバイダセキュアコンテナが、ユーザホームネットワーク5のレシーバ51により受信される。この処理の詳細は、図40のフローチャートに示されている。すなわち、ステップS241において、レシーバ51の相互認証モジュール71は、通信部61を介して、サービスプロバイダ3の相互認証部45と相互認証し、相互認証できたとき、通信部61は、相互認証したサービスプロバイダ3から、サービスプロバイダセキュアコンテナを受信する。相互認証できなかった場合、処理は終了されるが、この例の場合、相互認証されたものとし、ステップS242に進む。

ステップS242において、レシーバ51の通信部61は、ステップS241で相互認証したサービスプロバイダ3から、公開鍵証明書を受信する。

ステップS243において、レシーバ51の復号／暗号化モジュール74は、ステップS241で受信したサービスプロバイダセキュアコンテナに含まれる署名を検証し、改竄がなかったか否かを検証する。ここで、改竄が発見された場合、処理は終了するが、この例の場合、改竄が発見されなかったものとし、ステップS244に進む。

ステップS244において、レシーバ51の記憶モジュール73に記憶されている基準情報51に基づいて利用条件を満たすUCPと価格条件を満たすPTが選択され、表示制御部67を介して、図示せず表示部に表示される。ユーザは、表示されたUCPおよびPTの内容を参照して、図示せぬ操作部を操作し、UCPの1つの利用内容を選択する。これにより、入力制御部68は、操作部から入力された、ユーザの操作に対応する信号をSAM62に出力する。

この例の場合、基準情報 5 1 の「利用ポイント情報」には、200 ポイント以上の利用ポイントが設定されているものとされているので、UCPA が選択可能となり、また基準情報 5 1 の「決済ユーザ情報」には、ユーザは男性とされているので、PTA-1 の「価格条件 10」に設定された条件を満たす。そこで、この例の場合、UCPA に対応して作成された PTA-1, PTA-2 のうち、PTA-1 が選択され、UCPA および PTA-1 の内容が、表示部に表示される。また、この例の場合、ユーザは、UCPA の利用内容 13 (PTA-1 の価格内容 13) を選択したものとする。

ステップ S 2 4 5 において、レシーバ 5 1 の SAM 6 2 の課金処理モジュール 7 2 は、ステップ S 2 4 4 で選択された、UCPA の「利用内容 13」の内容 (PTA-1 の「価格内容 13」の内容) に基づいて、UCSA および課金情報 A を作成する。

ステップ S 2 4 6 において、サービスプロバイダセキュアコンテナに含まれる、コンテンツ A (コンテンツ鍵 K c o A で暗号化されている)、UCPA、PTA-1, PTA-2、およびコンテンツプロバイダ 2 の署名は取り出され、HDD 5 2 に出力され、記憶される。ステップ S 2 4 7 において、復号/暗号化ユニット 7 4 の復号ユニット 9 1 は、サービスプロバイダセキュアコンテナに含まれるコンテンツ鍵 K c o A (配送用鍵 K d で暗号化されている) を、記憶モジュール 7 3 に記憶されている配送用鍵 K d で復号する。

ステップ S 2 4 8 において、復号/暗号化ユニット 7 4 の暗号化ユニット 9 3 は、ステップ S 2 4 7 で復号されたコンテンツ鍵 K c o A を、記憶モジュール 7 3 に記憶されている保存用鍵 K s a v e で暗号化する。

ステップ S 2 4 9 において、SAM 6 2 のデータ検査モジュール 7 5 は、ステップ S 2 4 8 で保存用鍵 K s a v e で暗号化されたコンテンツ鍵 K c o A、およびステップ S 2 4 5 で作成された UCSA が対応して記憶される、外部記憶部 6 3 の利用情報記憶部 6 3 A の空き領域を有するブロック B P を検出する。この例の場合、利用情報記憶部 6 3 A のブロック B P-1 が検出される。なお、図 2 2

の利用情報記憶部 63Aにおいて、そのブロックBP-1の利用情報用メモリ領域RP-3にコンテンツ鍵KcoAおよびUCSAが、すでに記憶されているように示されているが、この例の場合、この時点において、それらは記憶されておらず、ブロックBP-1の利用情報用メモリ領域RP-3は、空いており、所定の初期情報が記憶されているものとする。

ステップS250において、レシーバ51のデータ検査モジュール75は、ステップS249で検出したブロックBP-1のデータ（利用情報用メモリ領域RP-1乃至RP-Nに記憶されている全てのデータ）にハッシュ関数を適用してハッシュ値を得る。次に、ステップS251において、データ検査モジュール75は、ステップS250で得られたハッシュ値と、記憶モジュール73に記憶されているブロックBP-1に対応する検査値HP-1とを比較し、値が一致するか否かを判定し、一致すると判定した場合、そのブロックBP-1のデータは改竄されていないので、ステップS252に進む。

ステップS252において、レシーバ51のSAM62は、利用情報（ステップS248で、保存用鍵Ksaveで暗号化されたコンテンツ鍵KcoA、およびステップS245で作成されたUCSA）を、利用情報記憶部63A（外部記憶部63）のブロックBP-1の利用情報用メモリ領域RP-3に記憶させる。

ステップS253において、レシーバ51のデータ検査モジュール75は、ステップS252で利用情報が記憶された利用情報用メモリ領域RP-3が属する、利用情報記憶部63AのブロックBP-1のデータにハッシュ関数を適用してハッシュ値を算出し、ステップS254において、記憶モジュール73に記憶されている検査値HP-1に上書きする。ステップS255において、課金処理モジュール72は、ステップS245で作成した課金情報Aを記憶モジュール73に記憶させ、処理は終了する。

ステップS251において、算出されたハッシュ値と検査値HP-1とが一致しないと判定された場合、ブロックBP-1のデータは改竄されているので、手続きは、ステップS256に進み、データ検査モジュール75は、外部記憶部6

3の利用情報記憶部63Aの全てのブロックBPを調べたか否かを判定し、外部記憶部63の全てのブロックBPを調べていないと判定した場合、ステップS257に進み、利用情報記憶部63Aの、調べていない（空きを有する他の）ブロックBPを検索し、ステップS250に戻り、それ以降の処理が実行される。

ステップS256において、外部記憶部63の利用情報記憶部63Aの全てのブロックBPが調べられたと判定された場合、利用情報を記憶できるブロックBP（利用情報用メモリ領域RP）は存在しないので、処理は終了する。

このように、サービスプロバイダセキュアコンテナが、レシーバ51により受信されると、処理は終了し、図33のステップS15に進む。

#### （6-4）コンテンツの再生処理

ステップS15において、供給されたコンテンツAが、レシーバ51において利用される。なお、この例の場合、図40のステップS224で選択されたUCPAの利用内容13によれば、コンテンツAは、再生して利用される。そこで、ここでは、コンテンツAの再生処理について説明する。この再生処理の詳細は、図41のフローチャートに示されている。

ステップS261において、レシーバ51のデータ検査モジュール75は、図40のステップS252で、コンテンツ鍵KcoA（保存用鍵Ksaveで暗号化されている）およびUCSAが記憶された利用情報用メモリ領域RP-3が属する、外部記憶部63の利用情報記憶部63AのブロックBP-1のデータにハッシュ関数を適用してハッシュ値を算出する。

ステップS262において、レシーバ51のデータ検査モジュール75は、ステップS261において算出したハッシュ値が、図40のステップS253で算出し、ステップS254で記憶モジュール73に記憶させたハッシュ値（検査値HP-1）と一致するか否かを判定し、一致すると判定した場合、ブロックBP-1のデータは改竄されていないので、ステップS263に進む。

ステップS263において、UCSA（図21）の「利用内容」の「パラメータ」に示されている情報に基づいて、コンテンツAが利用可能か否かが判定され

る。例えば、「利用内容」の「形式」が、「期間制限再生」とされているUCSにおいては、その「パラメータ」には、その開始期間（時刻）と終了期間（時刻）が記憶されているので、この場合、現在の時刻が、その範囲内にあるか否かが判定される。すなわち、現在時刻が、その範囲内にあるとき、そのコンテンツの利用が可能であると判定され、範囲外にあるとき、利用不可と判定される。また、「利用内容」の「形式」が、所定の回数に限って再生（複製）する利用形式とされているUCSにおいては、その「パラメータ」には、残された利用可能回数が記憶されている。この場合、「パラメータ」に記憶されている利用可能回数が0回でないとき、対応するコンテンツの利用が可能であると判定され、利用可能回数が0回であるとき、利用不可と判定される。

なお、UCSAの「利用内容」の「形式」は、「期間制限再生」とされているが、この場合、現在の時刻が、その期間内であるとし、ステップS263において、コンテンツAが利用可能であると判定され、ステップS264に進む。

ステップS264において、レシーバ51の課金モジュール72は、UCSAを更新する。UCSAには、更新すべき情報は含まれていないが、例えば、「利用内容」の「形式」が所定の回数に限って再生する利用形式とされている場合、その「パラメータ」に記憶されている、再生可能回数が1つだけデクリメントされる。

次に、ステップS265において、レシーバ51のSAM62は、ステップS264で更新されたUCSA（この例の場合には、実際は、更新されていない）を、外部記憶部63の利用情報記憶部63AのブロックBP-1の利用情報用メモリ領域RP-3に記憶させる。ステップS266において、データ検査モジュール75は、ステップS265でUCSAが記憶された、外部記憶部63の利用情報記憶部63AのブロックBP-1のデータにハッシュ関数を適用して、ハッシュ値を算出し、記憶モジュール73に記憶されている検査値HP-1に上書きする。

ステップS267において、SAM62の相互認証モジュール71と、伸張部

64の相互認証モジュール101は、相互認証し、SAM62および伸張部64は、一時鍵Ktempを共有する。この認証処理は、図35乃至図37を参照して説明した場合と同様であるので、ここでは説明を省略する。相互認証に用いられる乱数R1、R2、R3、またはその組み合わせが、一時鍵Ktempとして用いられる。

ステップS268において、復号／暗号化モジュール74の復号ユニット91は、図40のステップS252で外部記憶部63の利用情報記憶部63AのブロックBP-1（利用情報用メモリ領域RP-3）に記憶されたコンテンツ鍵KcoA（保存用鍵Ksaveで暗号化されている）を、記憶モジュール73に記憶された保存用鍵Ksaveで復号する。

次に、ステップS269において、復号／暗号化モジュール74の暗号化ユニット93は、復号されたコンテンツ鍵KcoAを一時鍵Ktempで暗号化する。ステップS270において、SAM62は、一時鍵Ktempで暗号化されたコンテンツ鍵KcoAを伸張部64に送信する。

ステップS271において、伸張部64の復号モジュール102は、コンテンツ鍵KcoAを一時鍵Ktempで復号する。ステップS272において、伸張部64は、インタフェース66を介して、HDD52に記録されたコンテンツA（コンテンツ鍵Kcoで暗号化されている）を受け取る。ステップS273において、伸張部64の復号モジュール103は、コンテンツA（コンテンツ鍵Kcoで暗号化されている）をコンテンツ鍵KcoAで復号する。

ステップS274において、伸張部64の伸張モジュール104は、復号されたコンテンツAをATRA2などの所定の方式で伸張する。ステップS275において、伸張部64のウォータマーク付加モジュール105は、伸張されたコンテンツAにレシーバ51を特定する所定のウォータマーク（電子透かし）を挿入する。ステップS276において、コンテンツAは、図示せぬスピーカなどに出力され、処理は終了する。

ステップS262において、ステップS261において算出されたハッシュ値



が、レシーバ51の記憶モジュール73に記憶されたハッシュ値と一致しないと判定された場合、またはステップS263において、コンテンツが利用不可と判定された場合、ステップS277において、SAM62は、表示制御部67を介して、図示せぬ表示部にエラーメッセージを表示させる等の所定のエラー処理を実行し、処理は終了する。

このようにして、レシーバ51において、コンテンツAが再生（利用）されたとき、処理は終了し、図33の処理も終了する。

#### （6-5）決済処理

次に、レシーバ51において計上された課金を決済する場合の処理手順を、図42のフローチャートを参照して説明する。なお、この処理は、計上された課金が所定の上限額（正式登録時の上限額または仮登録時の上限額）を越えた場合、または配送用鍵Kdのバージョンが古くなり、例えば、図40のステップS247で、コンテンツ鍵Kco（配送用鍵Kdで暗号化されている）を復号することができなくなった場合（サービスプロバイダセキュアコンテナを受信することができなくなった場合）に開始される。

ステップS301において、レシーバ51とEMDサービスセンタ1との相互認証が行われる。この相互認証は、図35乃至図37を参照して説明した場合と同様の処理であるので、その説明は省略する。

次に、ステップS302において、レシーバ51のSAM62は、EMDサービスセンタ1のユーザ管理部18（図3）に証明書を送信する。ステップS303において、レシーバ51のSAM62は、決済される課金（課金情報）に対応するUCPを、ステップS301でEMDサービスセンタ1と共有した一時鍵Ktempで暗号化し、記憶モジュール73に記憶されている、配送用鍵Kdのバージョン、課金情報（例えば、図23の課金情報A）、および登録リストとともに、EMDサービスセンタ1に送信する。

ステップS304において、EMDサービスセンタ1のユーザ管理部18は、ステップS303で、レシーバ51から送信された情報を受信し、復号した後、

EMDサービスセンタ1のユーザ管理部18が、登録リストの「状態フラグ」に”停止”が設定されるべき不正行為がレシーバ51において存在するか否かを確認する。

ステップS305において、EMDサービスセンタ1の課金請求部19は、ステップS303で受信された課金情報を解析し、ユーザの支払い金額を算出する処理等を行う。次に、ステップS306において、ユーザ管理部18は、ステップS305における処理により、決済が成功したか否かを確認する。

次に、ステップS307において、EMDサービスセンタ1のユーザ管理部18は、ステップS304における確認結果、およびステップS306における確認結果に基づいて、レシーバ51の登録条件を設定し、それに署名を付して、レシーバ51の登録リストを作成する。

例えば、ステップS304で、不正行為が確認された場合、「状態フラグ」には”停止”が設定され、この場合、今後、全ての処理が停止される。すなわち、EMDシステムからのサービスを一切受けることができなくなる。また、ステップS306で、決済が成功しなかったことが確認された場合、「状態フラグ」には”制限あり”が設定され、この場合、すでに購入したコンテンツを再生する処理は可能とされるが、新たにコンテンツを購入する処理は実行できなくなる。

次に、ステップS308に進み、EMDサービスセンタ1のユーザ管理部18は、最新バージョンの配送用鍵Kd（3ヶ月分の最新バージョンの配送用鍵Kd）およびステップS307で作成された登録リストを、一時鍵Ktempで暗号化し、レシーバ51に送信する。

ステップS309において、レシーバ51のSAM62は、EMDサービスセンタ1から送信された配送用鍵Kdおよび登録リストを、通信部61を介して受信し、復号した後、記憶モジュール73に記憶させる。このとき、記憶モジュール73に記憶されていた課金情報は消去され、登録リストおよび配送用鍵Kdが更新される。また、このとき、受信された登録リストの登録リスト署名が検証され、登録リストが改竄されていないとが確認される。この署名の確認処理は、図

37のステップS83における処理と同様であるので、その説明は省略する。

(6-6) 権利の再購入処理 (レシーバ51)

次に、コンテンツを利用する権利を再購入する場合のレシーバ51の処理手順を、図43のフローチャートを参照して説明する。ここでは、コンテンツAを”期間制限再生”の利用形式で利用することができる権利を保持している(すでに購入している)レシーバ51が、”買い取り再生”の利用形式で利用する権利を購入する場合を例として説明する。

ステップS401において、HDD52に記憶されているコンテンツA、UCPA、およびPTA-1, A-2が改竄されているか否かが判定される。具体的には、レシーバ51の復号/暗号化モジュール74が、図40のステップS246で、コンテンツA、UCPA、およびPTA-1, A-2とともに、HDD52に記憶させた署名を、公開鍵暗号の公開鍵で復号し、その結果(ハッシュ値)と、コンテンツA、UCPA、およびPTA-1, A-2の全体のハッシュ値とが、等しいか否かを判定する。それらの値が等しいと判定された場合、データは、改竄されていないと判定され、ステップS402に進む。

ステップS402において、コンテンツAに対応する利用情報(コンテンツ鍵KcoAおよびUCSA)が改竄されているか否かが判定される。具体的には、レシーバ51のデータ検査モジュール75が、コンテンツAの利用情報が記憶されている、外部記憶部63の利用情報記憶部63AのブロックBP(この例の場合、ブロックBP-1)のデータにハッシュ関数を適用してハッシュ値を算出し、それが、記憶モジュール73に記憶されている、そのブロックBPに対応する検査値HP(この例の場合、検査値HP-1)と等しいか否かを判定する。それらの値が等しいと判定された場合、利用情報が改竄されていないと判定され、ステップS403に進み、レシーバ51のSAM62は、外部記憶部63の利用情報記憶部63Aから、UCSAを取り出す。

次に、ステップS404において、SAM62は、UCSと課金情報を作成する。具体的には、表示制御部67が、UCPA、PTA-1, A-2、およびU

CSAの内容を、図示せぬ表示部に表示する。そこで、ユーザFは、UCSAの「利用内容」の「形式」に、“期限制限再生”（形式13）が設定されていることから、UCPAの「利用内容15」の「形式15」での利用が可能であること、その価格（PTA-1の価格内容15）などを確認する。そして、この例の場合、ユーザFは、UCPAの「利用内容15」およびPTA-1を選択する操作を、レシーバ51の図示せぬ操作部に対して行う。これにより、入力制御部68は、ユーザの操作に対応する信号（UCPAの「利用内容15」のIDとPTA-1のID）を操作部から受信し、それをSAM62に出力する。その後、SAM62の課金モジュール72は、入力制御部68からのUCPAの「利用内容1」のIDとPTA-1のIDに基づいて、図44および図45に示すように、「利用内容」のUCPAの「利用形式15」の内容が設定されたUCSBおよび課金情報Bを作成する。

次に、ステップS405において、レシーバ51のSAM62は、ステップS404で作成された課金情報Bを、記憶モジュール73に記憶させ、ステップS406において、ステップS404で作成されたUCSBを、UCSAに換えて外部記憶部63の利用情報記憶部63Aに記憶させる。

ステップS407において、レシーバ51のデータ検査モジュール75は、ステップS406で、UCSBが記憶された、外部記憶部63の利用情報記憶部63AのブロックBPのデータにハッシュ関数を適用してハッシュ値を算出する。そして、ステップS408において、データ検査モジュール75は、算出したハッシュ値を記憶モジュール73に記憶されている、そのブロックBPに対応する検査値HPに上書きする。その後、処理は終了される。

ステップS401において、コンテンツA、UCPA、およびPTA-1、A-2が改竄されていると判定された場合、またはステップS402において、コンテンツ鍵KcoAおよびUCSAが改竄されていると判定された場合、処理は終了する。

以上のようにして、レシーバ51は、コンテンツAを利用する権利の再購入す

る。

なお、ステップS 4 0 3で作成された課金情報Bに基づいて計上された課金は、図4 2のフローチャートで説明した決済処理により決済される。すなわち、この例の場合、ユーザは、コンテンツAを、新規に購入する場合の買い取り価格（2 0 0 0円）比べ、割安の価格（1 9 8 0円）で購入することができる。

#### （6－7）権利の再購入処理（レシーバ3 0 1）

次に、レシーバ3 0 1において権利を再購入する場合の処理手順を、図4 6のフローチャートを参照して説明する。レシーバ5 1が、図4 3のフローチャートで説明した処理により、コンテンツAをレシーバ5 1において” 買い取り再生” の利用形式で利用する権利を有している状態で、さらにコンテンツAをレシーバ3 0 1において” 買い取り再生” で利用する権利を購入する場合を例として説明する。

ステップS 4 2 1において、レシーバ5 1（コンテンツを供給する機器）のSAM 6 2およびレシーバ3 0 1（コンテンツの供給を受ける機器）のSAM 3 1のそれぞれは、各自が保持する登録リストの登録条件を参照し、再購入処理の実行が可能であるか否かを確認する。具体的には、コンテンツの供給機器のSAM（この例の場合、レシーバ5 1のSAM 6 2）は、自分の登録リストに、コンテンツの供給を受ける機器（この例の場合、レシーバ3 0 1）の登録条件が設定されており、またその「コンテンツ供給機器」に自分自身のSAMのIDが設定されているか否かを確認する。コンテンツの供給を受ける機器は、登録リストの自分自身の登録条件の「コンテンツ供給機器」に、コンテンツを供給する機器が設定されているか否かを確認する。

この例の場合、ここでは、レシーバ5 1において、レシーバ5 1の登録リストに、レシーバ3 0 1の登録リストが設定され、かつその「コンテンツ供給機器」にSAM 6 2のIDが設定され、そしてレシーバ3 0 1において、レシーバ3 0 1の登録リストのレシーバ3 0 1の登録条件の「コンテンツ供給機器」にSAM 6 2のIDが設定されているので、再購入処理の実行が可能であることが確認さ

れ、ステップS 4 2 2に進む。

ステップS 4 2 2において、レシーバ5 1とレシーバ3 0 1との相互認証が行われる。この相互認証は、図3 7を参照して説明した場合と同様であるので、その説明は省略するが、これにより、レシーバ5 1とレシーバ3 0 1は、一時鍵K t e m pを共有する。

ステップS 4 2 3において、レシーバ5 1は、HDD 5 2に記憶されているコンテンツA、UCPA、およびPTA-1、A-2が改竄されているか否かを判定する。具体的には、レシーバ5 1の復号/暗号化モジュール7 4が、図4 0のステップS 2 4 6で、コンテンツA、UCPA、およびPTA-1、A-2とともに、HDD 5 2に記憶された署名を、公開鍵暗号の公開鍵で復号し、その結果（ハッシュ値）と、コンテンツA、UCPA、およびPTA-1、A-2の全体のハッシュ値とが、等しいか否かを判定する。それらの値が等しいと判定された場合、データは改竄されていないと判定され、ステップS 4 2 4に進む。

ステップS 4 2 4において、レシーバ5 1は、コンテンツAに対応する利用情報（コンテンツ鍵K c o AおよびUCSB）が改竄されているか否かを判定する。

具体的には、レシーバ5 1のデータ検査モジュール7 5が、コンテンツAの利用情報が記憶されている、外部記憶部6 3の利用情報記憶部6 3 AのブロックBP（この例の場合、ブロックBP-1）のデータにハッシュ関数を適用してハッシュ値を算出し、それが、記憶モジュール7 3に記憶されている、そのブロックBPに対応する検査値HP（この例の場合、検査値HP-1）と等しいか否かを判定する。それらの値が等しいと判定された場合、利用情報が改竄されていないと判定され、ステップS 4 2 5に進む。

ステップS 4 2 5において、レシーバ5 1は、UCSと課金情報を作成する。具体的には、表示制御部6 7は、UCPA、PTA-1、A-2、およびUCSBの内容を、図示せぬ表示部に表示する。そこで、ユーザF（または、ユーザA）は、UCSBの「利用内容」の「形式」に、“形式1 3→形式1 1”が設定

されていることから（現在、コンテンツAを” 買い取り再生” で利用する権利を有していることから）、UCPAの「利用内容16」の「形式16」での利用が可能であること、その価格（PTA-1の価格内容16）などを確認する。そして、この例の場合、ユーザFは、UCPAの「利用内容16」およびPTA-1を選択する操作を、図示せぬ操作部に対して行う。これにより、入力制御部68は、ユーザFの操作に対応する信号（UCPAの「利用内容16」のIDとPTA-1のID）を操作部から受信し、それをSAM62に出力する。その後、SAM62の課金モジュール72は、入力制御部68からのUCPAの「利用内容16」のIDとPTA-1のIDに基づいて、図47および図48に示すように、「利用内容」にUCPAの「利用内容16」の内容が設定されたUCSCおよび課金情報Cを作成する。

次に、ステップS426において、HDD52に記憶されている、コンテンツA、UCPA、およびPTA-1、A-2、ステップS423で、改竄されていないことが確認されたコンテンツ鍵KcoA、ステップS425で作成されたUCSB、および署名（UCSBおよびコンテンツ鍵KcoAに対する署名）が、レシーバ301に送信される。なお、UCSB、コンテンツ鍵KcoA、および署名は、SAM62が、一時鍵Ktempで暗号化し、通信部65を介して、レシーバ301に送信する。また、UCSBは、レシーバ301に送信された後、権利の増殖を防止するために消去される。

コンテンツの供給を受ける機器であるレシーバ301は、上述したように、UCP、PT、およびUCSの内容をユーザに表示する表示部や、利用内容等を選択することができる操作部を有しておらず、そのため、UCSや課金情報を自分自身で作成することができない。そこで、このような場合、ステップS425において、コンテンツを供給する機器であるレシーバ51により、UCSおよび課金情報が作成される。また、レシーバ301は、上述したように、課金処理を実行することができないので、作成された課金情報は、ステップS426で、レシーバ301に送信されず、レシーバ51により保持され、レシーバ51により処

理される。

次に、ステップS 4 2 7において、レシーバ3 0 1のSAM 3 1 1は、ステップS 4 2 6で、レシーバから送信されてきたデータを受信する。なお、一時鍵K t e m pで暗号化された送信されてきたUCSB、コンテンツ鍵K c o A、および署名は、一時鍵K t e m pで復号される。

ステップS 4 2 8において、レシーバ3 0 1の復号／暗号化モジュール3 2 4は、ステップS 4 2 7で受信されたUCSBおよびコンテンツ鍵K c o Aに付された署名を確認し、UCSBおよびコンテンツ鍵K c o Aが改竄が改竄されているか否かを判定する。この署名の確認は、図3 7のステップS 8 3における処理と同様であるので、その説明は省略する。

ステップS 4 2 8において、UCSBおよびコンテンツ鍵K c o Aが改竄されていないと判定された場合、ステップS 4 2 9に進み、レシーバ3 0 1のSAM 3 1 1は、ステップS 4 2 7で受信されたコンテンツA、UCPA、およびPTA-1, PTA-2を記憶モジュール3 2 3に記憶させる。

ステップS 4 3 0において、レシーバ3 0 1のデータ検査モジュール3 2 5は、コンテンツ鍵K c o Aを記憶する、外部記憶部3 1 2の利用情報記憶部3 1 2 AのブロックBPを検出する。次に、ステップS 4 3 1において、レシーバ3 0 1のデータ検査モジュール3 2 5は、ステップS 4 3 0で検出した、利用情報記憶部3 1 2 AのブロックBPのデータにハッシュ関数を適用してハッシュ値を算出し、記憶モジュール3 2 3に記憶されている、検出されたブロックBPに対応する検査値HPと一致しているか否かを判定する。それらの値が一致すると判定された場合、すなわち、ステップS 4 3 0で検出されたブロックBPが改竄されていない場合、ステップS 4 3 2に進み、データ検査モジュール3 2 5は、ステップS 4 2 7で受信されたUCSBおよびコンテンツ鍵K c o Aを、それぞれ対応させてブロックBPに記憶させる。

ステップS 4 3 3において、レシーバ3 0 1のデータ検査モジュール3 2 5は、ステップS 4 3 2で、UCSBおよびコンテンツ鍵K c o Aが記憶された外部



記憶部 3 1 2 の利用情報記憶部 3 1 2 A のブロック B P のデータにハッシュ関数を適用してハッシュ値を算出し、記憶モジュール 3 2 3 に記憶されている、そのブロック B P に対応する検査値 H P に上書きする。その後、処理は終了される。

ステップ S 4 2 8 において、レシーバ 5 1 からのデータが改竄されていると判定された場合、ステップ S 4 3 4 に進み、レシーバ 3 0 1 の S A M 3 1 1 は、その旨をレシーバ 5 1 に通知する等の処理を実行する。その後、ステップ S 4 2 4 に戻る。すなわち、これにより、コンテンツ A、U C P A、P T A - 1、A - 2、U C S B、コンテンツ鍵 K c o A、および署名が、再度、レシーバ 3 0 1 に送信される。なお、この例の場合、レシーバ 5 1 からのこの送信は、予め決められた回数だけ行われるものとし、その回数を越えた場合、処理は終了されるものとする。

ステップ S 4 2 1 で、再購入処理の実行が可能でないと判定された場合、ステップ S 4 2 3 で、コンテンツ A、U C P A、および P T A - 1、A - 2 が改竄されていると判定された場合、ステップ S 4 2 4 で、U C S B およびコンテンツ鍵 K c o A が改竄されていると判定された場合、またはステップ S 4 3 1 において、検出されたブロック B P が改竄されていると判定された場合、処理は終了される。

#### ( 6 - 8 ) 権利の再購入処理 ( レシーバ 2 0 1 )

次に、レシーバ 2 0 1 において権利を再購入する場合の処理手順を、図 4 9 のフローチャートを参照して説明する。レシーバ 5 1 が、図 4 3 のフローチャートで説明した処理により、コンテンツ A をレシーバ 5 1 において” 買い取り再生” の利用形式で利用する権利を有している状態で、さらにコンテンツ A をレシーバ 2 0 1 において” 買い取り再生” で利用する権利を購入する場合を例として説明する。

ステップ S 4 5 1 において、レシーバ 5 1 の S A M 6 2 およびレシーバ 2 0 1 の S A M 2 1 2 のそれぞれは、各自が保持する登録リストの登録条件を参照し、再購入処理の実行が可能か否かを確認する。なお、ここでの具体的な処理は、図

46のステップS421における場合と同様であるので、その説明は省略するが、この例の場合、再購入処理の実行が可能であると判定され、ステップS452に進む。

ステップS452において、レシーバ51とレシーバ201との相互認証が行われる。この相互認証は、図37を参照して説明した場合と同様であるので、その説明は省略するが、これにより、レシーバ51とレシーバ201は、一時鍵Ktempを共有する。

ステップS453において、コンテンツAに対応する利用情報（コンテンツ鍵KcoAおよびUCSB）が改竄されているか否かが判定される。具体的には、レシーバ51のデータ検査モジュール75が、コンテンツAの利用情報が記憶されている、外部記憶部63の利用情報記憶部63AのブロックBP（この例の場合、ブロックBP-1）のデータにハッシュ関数を適用してハッシュ値を算出し、それが、記憶モジュール73に記憶されている、そのブロックBPに対応する検査値HP（この例の場合、検査値HP-1）と等しいか否かを判定する。それらの値が等しいと判定された場合、利用情報が改竄されていないと判定され、ステップS454に進む。

ステップS454において、図40のステップS246で、レシーバ201のHDD52に記憶された、コンテンツA、UCPA、PTA-1、A-2、および署名（コンテンツA、UCPA、PTA-1、PTA-2に対する署名）、並びに、ステップS453で、改竄されていないことが確認された、UCSB、コンテンツ鍵KcoA、および署名（UCSBおよびコンテンツ鍵KcoAに対する署名）が、レシーバ201に送信される。なお、UCSB、コンテンツ鍵KcoA、および署名は、SAM62が、一時鍵Ktempで暗号化し、通信部65を介して、レシーバ201に送信する。

次に、ステップS455において、レシーバ201のSAM212は、ステップS454で、レシーバ51から送信されてきたデータを受信する。なお、一時鍵Ktempで暗号化されて送信されてきたUCSB、コンテンツ鍵KcoA、

および署名は、一時鍵  $K_{temp}$  で復号される。

ステップ S 4 5 6 において、レシーバ 2 0 1 の復号／暗号化モジュール 2 2 4 は、ステップ S 4 5 5 で受信された UCSB およびコンテンツ鍵  $K_{coA}$  の署名を確認し、UCSB およびコンテンツ鍵  $K_{coA}$  が改竄されているか否かを判定し、改竄されていないと判定した場合、ステップ S 4 5 7 に進む。この署名の確認は、図 3 7 のステップ S 8 3 における処理と同様であるので、その説明は省略する。

ステップ S 4 5 7 において、レシーバ 2 0 1 の復号／暗号化モジュール 2 2 4 は、ステップ S 4 5 5 で受信されたコンテンツ A、UCPA、および PTA-1, A-2 が改竄されているか否かを判定する。具体的には、レシーバ 2 0 1 の復号／暗号化モジュール 2 2 4 が、ステップ S 4 5 5 で受信された署名（コンテンツ A、UCPA、および PTA-1, A-2 に対する署名）を、公開鍵暗号の公開鍵で復号し、その結果（ハッシュ値）と、コンテンツ A、UCPA、および PTA-1, A-2 の全体のハッシュ値とが等しいか否かを判定する。それらの値が等しいと判定された場合、データは改竄されていないと判定され、ステップ S 4 5 8 に進む。

ステップ S 4 5 8 において、レシーバ 2 0 1 の SAM 2 1 2 は、ステップ S 4 5 5 で受信されたコンテンツ A、UCPA、および PTA-1, PTA-2 を、自分自身の署名を付して、HDD 2 0 2 に記憶させる。

ステップ S 4 5 9 において、レシーバ 2 0 1 のデータ検査モジュール 2 2 5 は、コンテンツ鍵  $K_{coA}$  を記憶する、外部記憶部 2 1 3 の利用情報記憶部 2 1 3 A のブロック BP を検出する。ステップ S 4 6 0 において、レシーバ 2 0 1 のデータ検査モジュール 2 2 5 は、ステップ S 4 5 9 で検出した、利用情報記憶部 2 1 3 A のブロック BP のデータにハッシュ関数を適用してハッシュ値を算出し、記憶モジュール 2 2 3 に記憶されている、検出されたブロック BP に対応する検査値 HP と一致しているか否かを判定する。それらの値が一致すると判定された場合、すなわち、ステップ S 4 5 9 で検出されたブロック BP が改竄されていない

い場合、ステップS 4 6 1に進む。

ステップS 4 6 1において、レシーバ2 0 1のSAM 2 1 2は、UCSと課金情報を作成する。具体的には、表示制御部2 1 7は、UCPA、PTA-1、A-2、およびUCSBの内容を、図示せぬ表示部に表示する。そこで、ユーザF（または、ユーザA）は、UCSBの「利用内容」の「形式」に、”形式1 3->形式1 1”が設定されていることから（現在、コンテンツAを”買い取り再生”で利用する権利を有していることから）、UCPAの「利用内容1 6」の「形式1 6」での利用が可能であること、その価格（PTA-1の価格内容1 6）などを確認する。そして、この例の場合、ユーザFは、UCPAの「利用内容1 6」およびPTA-1を選択する操作を、レシーバ2 0 1の図示せぬ操作部に対して行う。これにより、入力制御部2 1 8は、ユーザFの操作に対応する信号（UCPAの「利用内容1 6」のIDとPTA-1のID）を操作部から受信し、それをSAM 2 1 2に出力する。その後、SAM 2 1 2の課金モジュール2 2 2は、入力制御部2 1 8からのUCPAの「利用内容1 6」のIDとPTA-1のIDに基づいて、図5 0および図5 1に示すように、「利用内容」にUCPAの「利用内容1 6」に内容が設定されたUCSDおよび課金情報Dを作成する。なお、UCSDが作成された後、レシーバ5 1から供給されたUCSBは、権利の増殖を防止するために消去される。

次に、ステップS 4 6 2において、レシーバ2 0 1のSAM 2 1 2は、ステップS 4 6 1で作成された課金情報Dを、記憶モジュール2 2 3に記憶させる。

このように、レシーバ2 0 1は、表示部や操作部を有しているので、自分自身でUCSおよび課金情報を作成する。またレシーバ2 0 1は、課金処理を実行することができるので、作成した課金情報を保持し、所定のタイミングで、それを処理する。

ステップS 4 6 3において、レシーバ2 0 1のSAM 2 1 は、ステップS 4 6 1で作成されたUCSDを、コンテンツ鍵K c o Aと対応させて、外部記憶部2 1 3の利用情報記憶部2 1 3 Aの、ステップS 4 5 9で検出されたブロックBP

に記憶させる。

ステップS 4 6 4において、レシーバ2 0 1のデータ検査モジュール2 2 5は、ステップS 4 6 3で、UCSDおよびコンテンツ鍵K c o Aが記憶された外部記憶部2 1 3の利用情報記憶部2 1 3 AのブロックB Pのデータにハッシュ関数を適用してハッシュ値を算出し、記憶モジュール2 2 3に記憶されている、そのブロックB Pに対応する検査値H Pに上書きする。その後、処理は終了される。

ステップS 4 5 6において、レシーバ5 1からのデータが改竄されていると判定された場合、ステップS 4 6 5に進み、レシーバ2 0 1のSAM 2 1 2は、その旨をレシーバ5 1に通知する等の処理を実行する。その後、ステップS 4 5 4に戻る。すなわち、これにより、コンテンツA、UCPA、PTA-1, A-2、UCSB、コンテンツ鍵K c o A、および署名が、再度、レシーバ2 0 1に送信される。なお、この例の場合、レシーバ5 1からのこの送信は、予め決められた回数だけ行われるものとし、その回数を越えた場合、処理は終了されるものとする。

ステップS 4 5 1において、再購入処理の実行が可能でないと判定された場合、ステップS 4 5 3において、UCSBおよびコンテンツ鍵K c o Aが改竄されていると判定された場合、ステップS 4 5 7において、コンテンツA、UCPA、およびPTA-1, A-2が改竄されていると判定された場合、またはステップS 4 6 0において、検出されたブロックB Pが改竄されていると判定された場合、処理は終了される。

以上においては、レシーバ5 1が、レシーバ2 0 1に供給する（ステップS 4 5 4）場合と例として説明したが、レシーバ2 0 1は、それらを、別途（例えば、EMDサービスセンタ1から直接）取得するようにすることもできる。

また、以上においては、コンテンツを”期間制限再生”で利用する権利を有している状態において、”買い取り再生”で利用する権利を購入する場合、および”買い取り再生”で利用する権利を有している状態において、”買い取り再生”で利用する権利を再度（他の機器において）購入する場合を例として説明したが

、その他利用形式の組み合わせにおいても、適用することができる。

また、以上においては、再購入の権利の内容を示す、UCPの「利用内容」（例えば、利用内容15または利用内容16）が選択された場合、UCSの「利用内容」の「ID」に「利用内容15」または「利用内容16」のIDが設定されるようにしたが、このとき再購入される「利用内容11」のIDが設定されるようにすることもできる。

また、以上においては、SAMの、公開鍵Kpuおよび証明書が、SAM内に（記憶モジュールに）記憶されるようにしたが、HDDに記憶させておくこともできる。

なお、コンテンツは、音楽データを例に説明したが、音楽データに限らず、動画像データ、静止画像データ、文書データ、またはプログラムデータでもよい。その際、圧縮は、コンテンツの種類に適した方式、例えば、画像であればMPEG（Moving Picture Experts Group）などが利用される。ウォーターマークも、コンテンツの種類に適した形式のウォーターマークが利用される。

また、共通鍵暗号は、ブロック暗号であるDESを使用して説明したが、NTT（商標）が提案するFEAL、IDEA（International Data Encryption Algorithm）、または1ビット乃至数ビット単位で暗号化するストリーム暗号などでもよい。

さらに、コンテンツおよびコンテンツ鍵Kcoの暗号化は、共通鍵暗号方式を利用するとして説明したが、公開鍵暗号方式でもよい。

なお、本明細書において、システムとは、複数の装置により構成される装置全体を表すものとする。

また、上記したような処理を行うコンピュータプログラムをユーザに提供する提供媒体としては、磁気ディスク、CD-ROM、固体メモリなどの記録媒体の他、ネットワーク、衛星などの通信媒体を利用することができる。

上述の本発明の実施の形態のレシーバは、購入された権利の内容に基づいて再

購入することができる権利の内容を示す第2の利用内容を含む取扱方針を記憶するようにしたので、第2の利用内容、および第2の利用内容に対応する価格内容を特定する第2の使用許諾条件情報を作成することができる。

また、本発明の実施の形態のレシーバは、使用許諾条件情報を受信するようにしたので、その使用許諾条件情報により特定される利用内容に示される権利の内容に基づいて、情報を利用することができる。

また、本発明の実施の形態のレシーバは、権利の内容を示す第1の利用内容と、第1の利用内容に対応する価格内容を特定する使用許諾条件情報を作成するようにしたので、使用許諾条件情報を他の情報処理装置に送信することができる。

また、本発明の実施の形態のレシーバは、他の情報処理装置から送信されてきた、使用許諾条件情報に含まれる利用内容により特定される権利の内容に基づいて再購入される第2の利用内容と、第2の利用内容に対応する価格内容を特定する第2の使用許諾条件情報を作成するようにしたので、第2の利用内容に示される権利の内容に基づいて、情報を利用することができる。

#### 産業上の利用の可能性

本発明は、音楽データ、動画像データ、静止画像データ、文書データ、プログラムデータなどの情報を暗号化し、配信する情報処理システムに適應できる。

## 請 求 の 範 囲

1. 他の情報処理装置に接続され、暗号化されている情報を復号して利用する権利を購入する情報処理装置において、

購入した権利の内容を示す第1の利用内容、および上記第1の利用内容に対応する価格内容を特定する第1の使用許諾条件情報を作成する第1の作成手段と、

暗号化されている上記情報、上記第1の使用許諾条件情報、購入した上記権利の内容に基づいて再購入することができる権利の内容を示す第2の利用形式を含む取扱方針、上記第2の利用内容に対応する価格内容を含む価格情報、および暗号化されている上記情報を復号するために必要な鍵を記憶する記憶手段と、

上記他の情報処理装置を介して、権利の再購入が行われるとき、上記取扱方針と上記価格情報に基づいて、上記第2の利用内容、および上記第2の利用内容に対応する価格内容を特定する第2の使用許諾条件情報を作成する第2の作成手段と、

上記第2の作成手段により作成された上記第2の使用許諾条件情報、並びに上記記憶手段に記憶されている、暗号化されている上記情報および上記鍵を、上記他の情報処理装置に送信する送信手段と

を具備する情報処理装置。

2. 上記第2の作成手段により作成された上記第2の使用許諾条件情報に基づいて、上記情報を利用するための処理を実行する第1の実行手段

をさらに具備する請求の範囲第1項に記載の情報処理装置。

3. 上記第1の使用許諾条件情報および上記第2の使用許諾条件情報に対応する課金情報を作成する第3の作成手段と、

上記第3の作成手段により作成された上記課金情報に基づいて計上された課金を決済するための決済処理を実行する第2の実行手段と



をさらに具備する請求の範囲第 1 項に記載の情報処理装置。

4. 他の情報処理装置に接続され、暗号化されている情報を復号して利用する権利を購入する情報処理装置の情報処理方法において、

購入した権利の内容を示す第 1 の利用内容、および上記第 1 の利用内容に対応する価格内容を特定する第 1 の使用許諾条件情報を作成する第 1 の作成ステップと、

暗号化されている上記情報、上記第 1 の使用許諾条件情報、購入した上記権利の内容に基づいて再購入することができる権利の内容を示す第 2 の利用形式を含む取扱方針、上記第 2 の利用内容に対応する価格内容を含む価格情報、および暗号化されている上記情報を復号するために必要な鍵を記憶する記憶ステップと、

上記他の情報処理装置を介して、権利の再購入が行われるとき、上記取扱方針と上記価格情報に基づいて、上記第 2 の利用内容、および上記第 2 の利用内容に対応する価格内容を特定する第 2 の使用許諾条件情報を作成する第 2 の作成ステップと、

上記第 2 の作成ステップで作成された上記第 2 の使用許諾条件情報、並びに上記記憶ステップに記憶されている、暗号化されている上記情報および上記鍵を、上記他の情報処理装置に送信する送信ステップと

を具備する情報処理方法。

5. 他の情報処理装置に接続され、暗号化されている情報を復号して利用する権利を購入する情報処理装置に、

購入した権利の内容を示す第 1 の利用内容、および上記第 1 の利用内容に対応する価格内容を特定する第 1 の使用許諾条件情報を作成する第 1 の作成ステップと、

暗号化されている上記情報、上記第 1 の使用許諾条件情報、購入した上記権利の内容に基づいて再購入することができる権利の内容を示す第 2 の利用形式を含

む取扱方針、上記第 2 の利用内容に対応する価格内容を含む価格情報、および暗号化されている上記情報を復号するために必要な鍵を記憶する記憶ステップと、

上記他の情報処理装置を介して、権利の再購入が行われるとき、上記取扱方針と上記価格情報に基づいて、上記第 2 の利用内容、および上記第 2 の利用内容に対応する価格内容を特定する第 2 の使用許諾条件情報を作成する第 2 の作成ステップと、

上記第 2 の作成ステップで作成された上記第 2 の使用許諾条件情報、並びに上記記憶ステップに記憶されている、暗号化されている上記情報および上記鍵を、上記他の情報処理装置に送信する送信ステップと

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする提供媒体。

6. 他の情報処理装置に接続され、購入された権利に対応して、暗号化されている情報を復号して利用する情報処理装置において、

上記他の情報処理装置から送信されてきた、暗号化されている上記情報、暗号化されている上記情報を復号するために必要な鍵、および上記権利の内容を示す利用内容と上記利用内容に対応する価格内容を特定する使用許諾条件情報を受信する受信手段と、

上記使用許諾条件情報により特定される上記利用内容に示される上記権利の内容に基づいて、上記情報を利用するための処理を実行する実行手段と

を具備する情報処理装置。

7. 他の情報処理装置に接続され、購入された権利に対応して、暗号化されている情報を復号して利用する情報処理装置の情報処理方法において、

上記他の情報処理装置から送信されてきた、暗号化されている上記情報、暗号化されている上記情報を復号するために必要な鍵、および上記権利の内容を示す利用内容と上記利用内容に対応する価格内容を特定する使用許諾条件情報を受信

する受信ステップと、

上記使用許諾条件情報により特定される上記利用内容に示される上記権利の内容に基づいて、上記情報を利用するための処理を実行する実行ステップとを具備する情報処理方法。

8. 他の情報処理装置に接続され、購入された権利に対応して、暗号化されている情報を復号して利用する情報処理装置に、

上記他の情報処理装置から送信されてきた、暗号化されている上記情報、暗号化されている上記情報を復号するために必要な鍵、および上記権利の内容を示す利用内容と上記利用内容に対応する価格内容を特定する使用許諾条件情報を受信する受信ステップと、

上記使用許諾条件情報により特定される上記利用内容に示される上記権利の内容に基づいて、上記情報を利用するための処理を実行する実行ステップと

を具備する処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする提供媒体。

9. 他の情報処理装置に接続され、暗号化されている情報を復号して利用する権利を購入する情報処理装置において、

暗号化されている上記情報、購入することができる権利の内容を示す利用内容を含む取扱方針、上記利用内容に対応する価格内容を含む価格情報、および暗号化されている上記情報を復号するために必要な鍵を記憶する記憶手段と、

上記記憶手段に記憶されている上記取扱方針および上記価格情報に基づいて、上記利用内容、および上記利用内容に対応する価格内容を特定する使用許諾条件情報を作成する作成手段と、

上記他の情報処理装置において、権利の再購入が行われるとき、上記作成手段により作成された上記使用許諾条件情報、並びに上記記憶手段に記憶されている、暗号化されている上記情報および上記鍵を、上記他の情報処理装置に送信する

## 送信手段と

を具備する情報処理装置。

10. 他の情報処理装置に接続され、暗号化されている情報を復号して利用する権利を購入する情報処理装置の情報処理方法において、

暗号化されている上記情報、購入することができる権利の内容を示す利用内容を含む取扱方針、上記利用内容に対応する価格内容を含む価格情報、および暗号化されている上記情報を復号するために必要な鍵を記憶する記憶ステップと、

上記記憶ステップで記憶された上記取扱方針および上記価格情報に基づいて、上記利用内容、および上記利用内容に対応する価格内容を特定する使用許諾条件情報を作成する作成ステップと、

上記他の情報処理装置において、権利の再購入が行われるとき、上記作成ステップで作成された上記使用許諾条件情報、並びに上記記憶ステップで記憶された、暗号化されている上記情報および上記鍵を、上記他の情報処理装置に送信する送信ステップと

を具備する情報処理方法。

11. 他の情報処理装置に接続され、暗号化されている情報を復号して利用する権利を購入する情報処理装置に、

暗号化されている上記情報、購入することができる権利の内容を示す利用内容を含む取扱方針、上記利用内容に対応する価格内容を含む価格情報、および暗号化されている上記情報を復号するために必要な鍵を記憶する記憶ステップと、

上記記憶ステップで記憶された上記取扱方針および上記価格情報に基づいて、上記利用内容、および上記利用内容に対応する価格内容を特定する使用許諾条件情報を作成する作成ステップと、

上記他の情報処理装置において、権利の再購入が行われるとき、上記作成ステップにて作成された上記使用許諾条件情報、並びに上記記憶ステップに記憶され

ている、暗号化されている上記情報および上記鍵を、上記他の情報処理装置に送信する送信ステップと

を具備する処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする提供媒体。

12. 他の情報処理装置に接続され、購入した権利に対応して、暗号化されている情報を復号して利用する情報処理装置において、

上記他の情報処理装置から送信されてきた、暗号化されている上記情報、暗号化されている上記情報を復号するために必要な鍵、および所定の権利の内容を示す第1の利用形式、および上記第1の利用形式に対応する価格内容を特定する使用許諾条件情報を受信する受信手段と、

上記受信手段により受信された上記使用許諾条件情報により特定される上記第1の利用内容に示される上記権利の内容に基づいて再購入される権利の内容を示す第2の利用内容を含む取扱方針、および上記第2の利用内容に対応する価格内容を含む価格情報を記憶する記憶手段と、

上記記憶手段に記憶されている上記取扱方針および上記価格情報に基づいて、上記第2の利用内容、および上記第2の利用内容に対応する価格内容を特定する第2の使用許諾条件情報を作成する第1の作成手段と

を具備する情報処理装置。

13. 上記第1の作成手段により作成された上記第2の使用許諾条件情報に対応する課金情報を作成する第2の作成手段と、

上記第2の作成手段により作成された上記課金情報に基づいて計上された課金を決済するための決済処理を実行する実行手段と

をさらに具備する請求の範囲第12項に記載の情報処理装置。

14. 他の情報処理装置に接続され、購入した権利に対応して、暗号化されて

いる情報を復号して利用する情報処理装置の情報処理方法において、

上記他の情報処理装置から送信されてきた、暗号化されている上記情報、暗号化されている上記情報を復号するために必要な鍵、および所定の権利の内容を示す第 1 の利用形式、および上記第 1 の利用形式に対応する価格内容を特定する使用許諾条件情報を受信する受信ステップと、

上記受信ステップで受信された上記使用許諾条件情報により特定される上記第 1 の利用内容に示される上記権利の内容に基づいて再購入される権利の内容を示す第 2 の利用内容を含む取扱方針、および上記第 2 の利用内容に対応する価格内容を含む価格情報を記憶する記憶ステップと、

上記記憶ステップで記憶された上記取扱方針および上記価格情報に基づいて、上記第 2 の利用内容、および上記第 2 の利用内容に対応する価格内容を特定する第 2 の使用許諾条件情報を作成する第 1 の作成ステップと

を具備する情報処理方法。

15. 他の情報処理装置に接続され、購入した権利に対応して、暗号化されている情報を復号して利用する情報処理装置に、

上記他の情報処理装置から送信されてきた、暗号化されている上記情報、暗号化されている上記情報を復号するために必要な鍵、および所定の権利の内容を示す第 1 の利用形式、および上記第 1 の利用形式に対応する価格内容を特定する使用許諾条件情報を受信する受信ステップと、

上記受信ステップで受信された上記使用許諾条件情報により特定される上記第 1 の利用内容に示される上記権利の内容に基づいて再購入される権利の内容を示す第 2 の利用内容を含む取扱方針、および上記第 2 の利用内容に対応する価格内容を含む価格情報を記憶する記憶ステップと、

上記記憶ステップで記憶された上記取扱方針および上記価格情報に基づいて、上記第 2 の利用内容、および上記第 2 の利用内容に対応する価格内容を特定する第 2 の使用許諾条件情報を作成する第 1 の作成ステップと

を具備する処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする提供媒体。

**This Page Blank (uspto)**



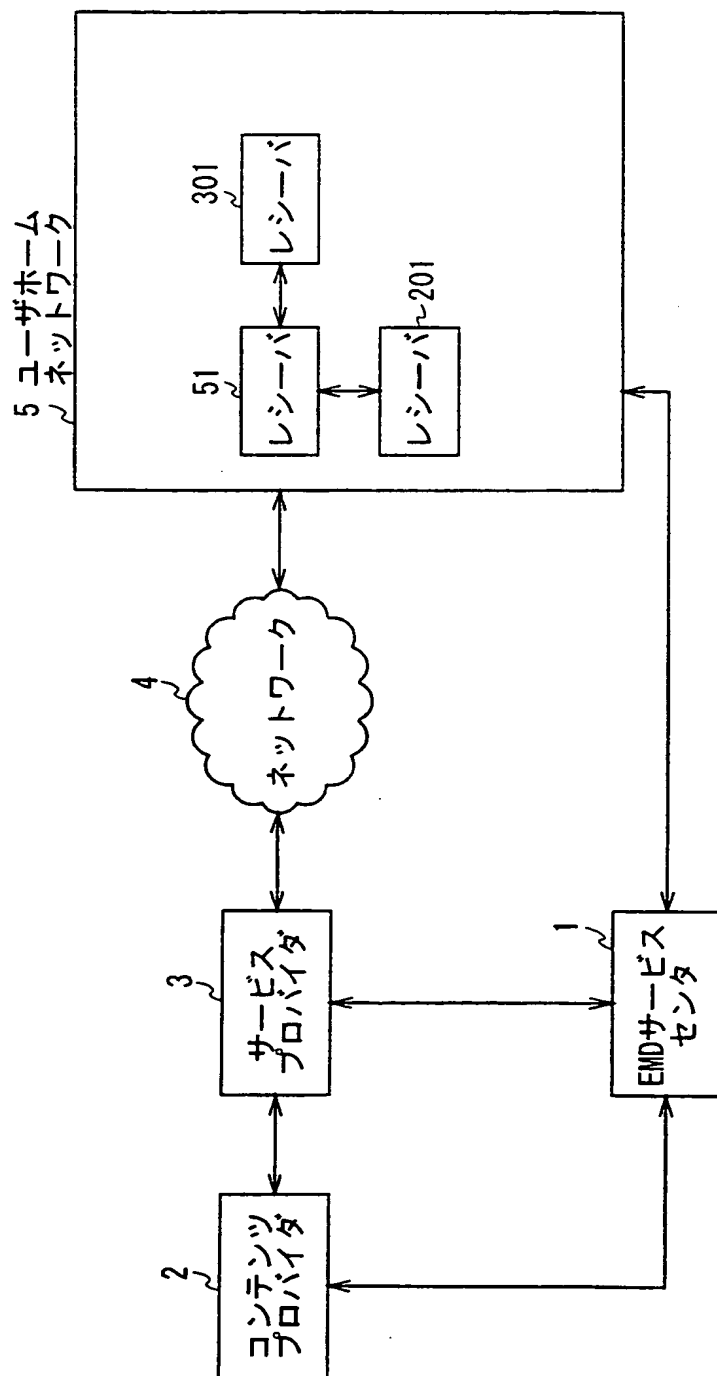


図 1

**This Page Blank (uspto)**

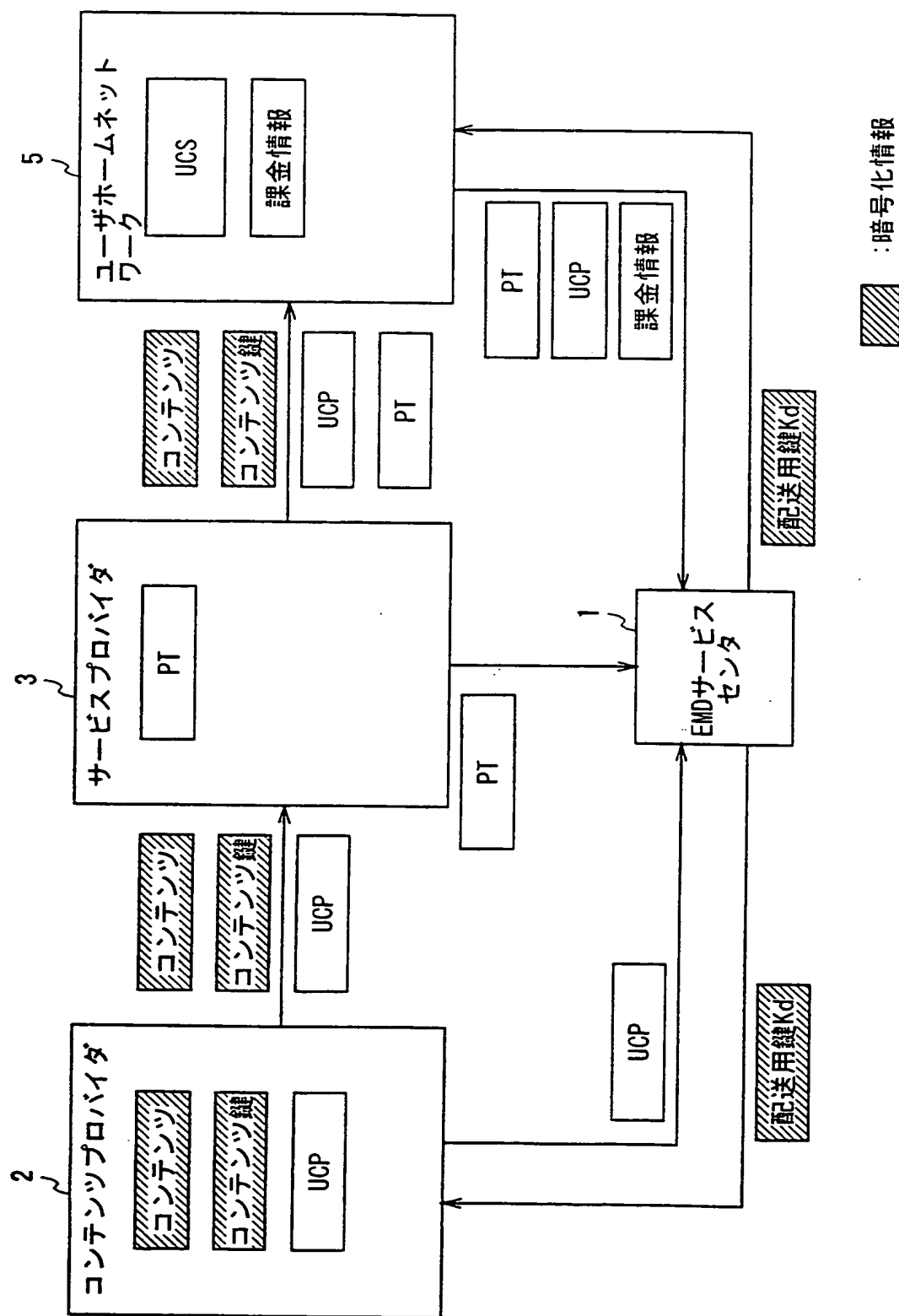
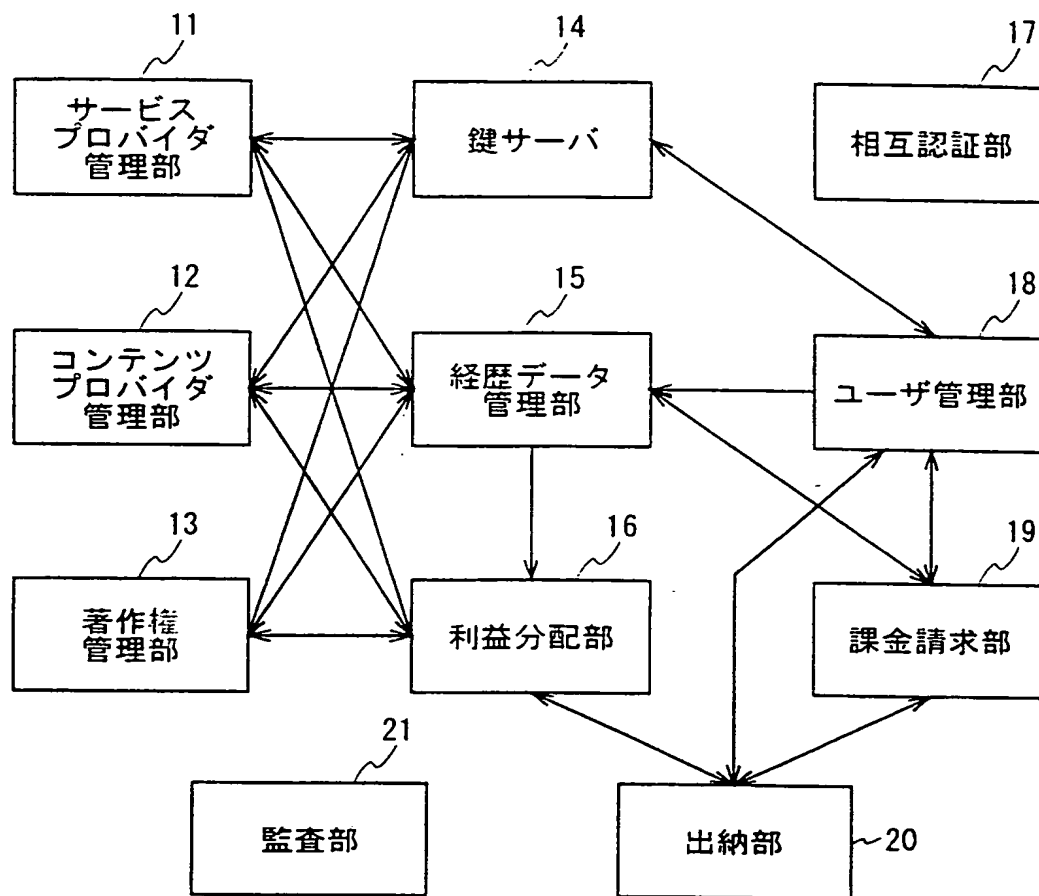


図 2

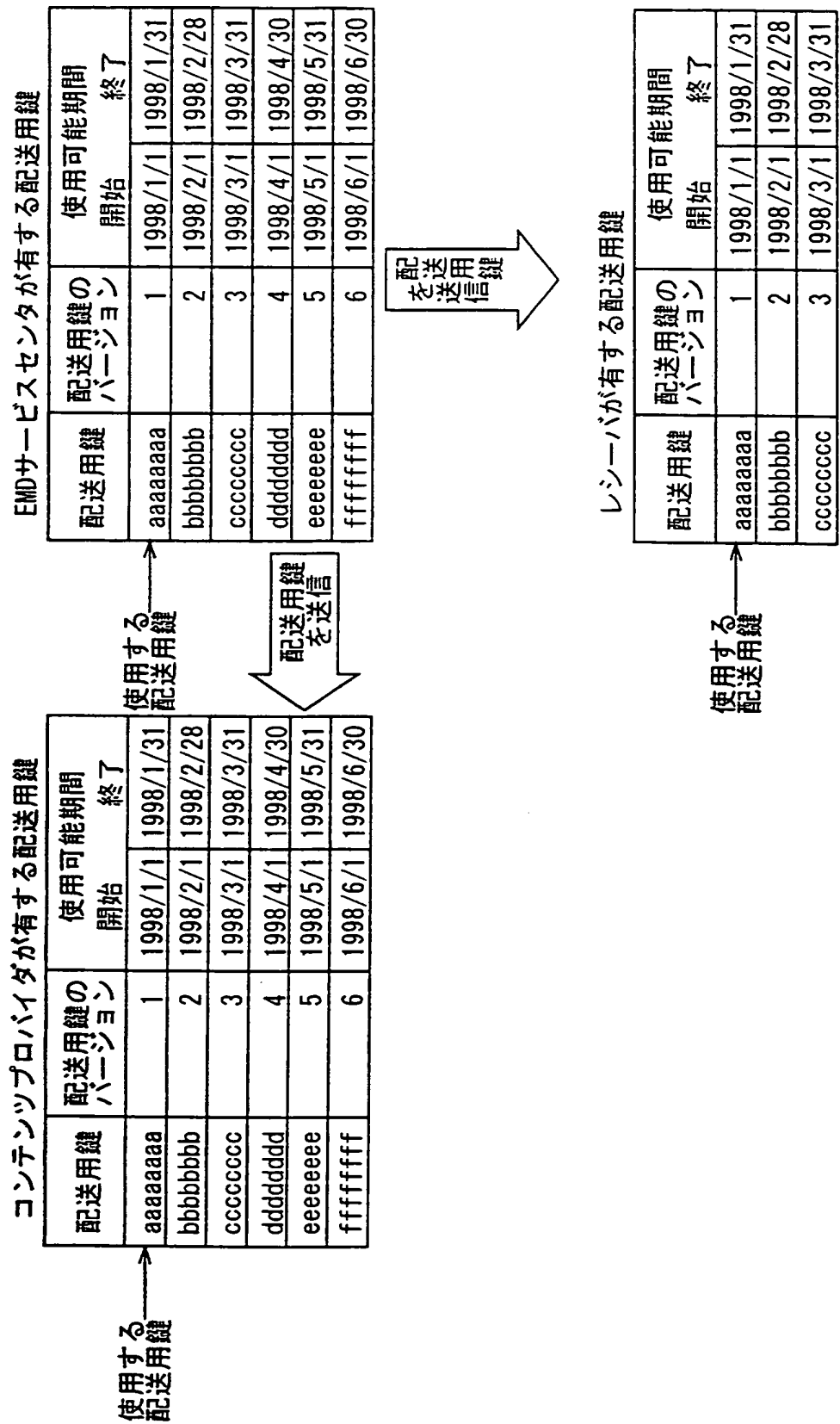
**This Page Blank (uspto)**



EMDサービスセンタ 1

図 3

**This Page Blank (uspto)**



**This Page Blank (uspto)**



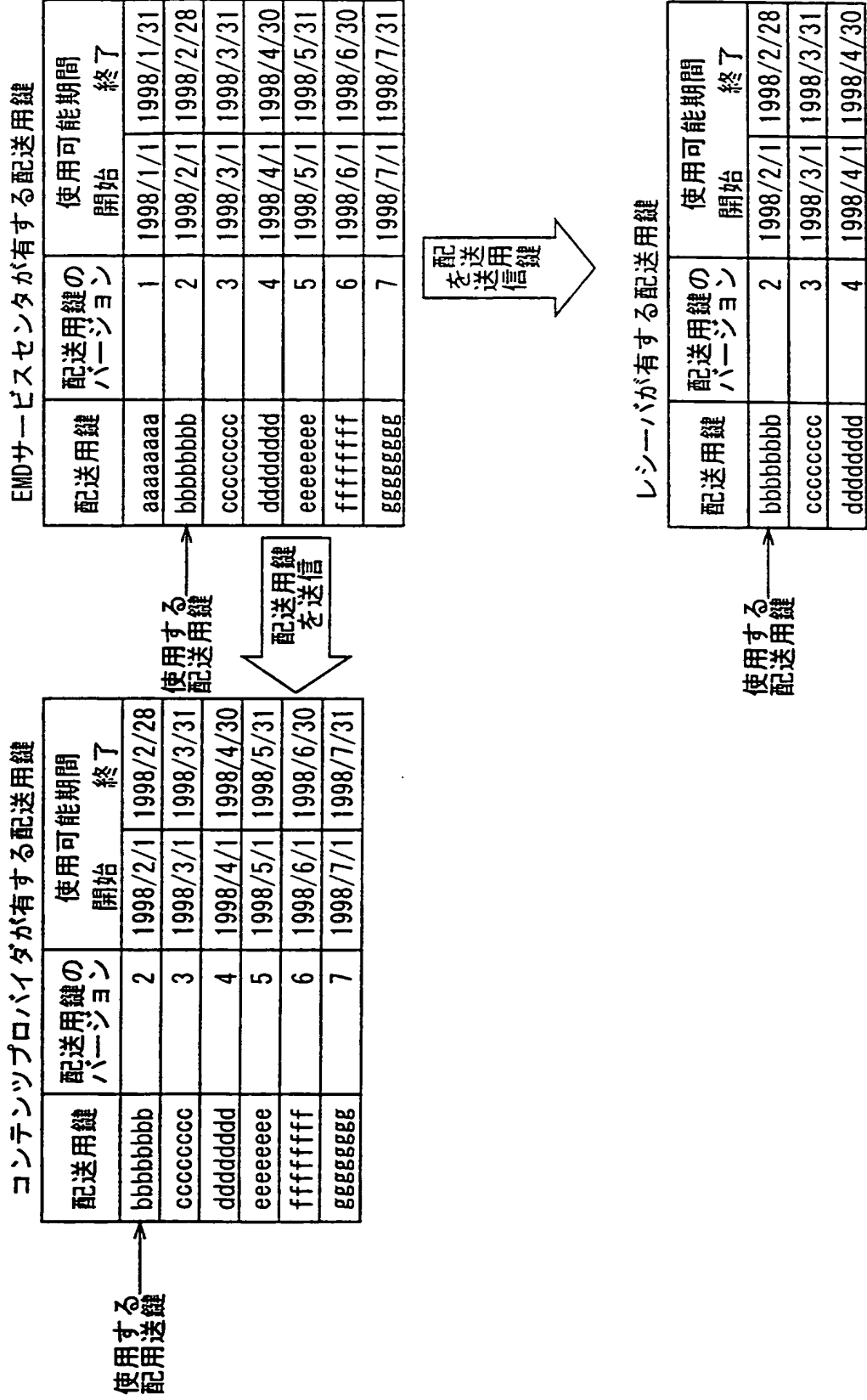


図 5

**This Page Blank (uspto)**

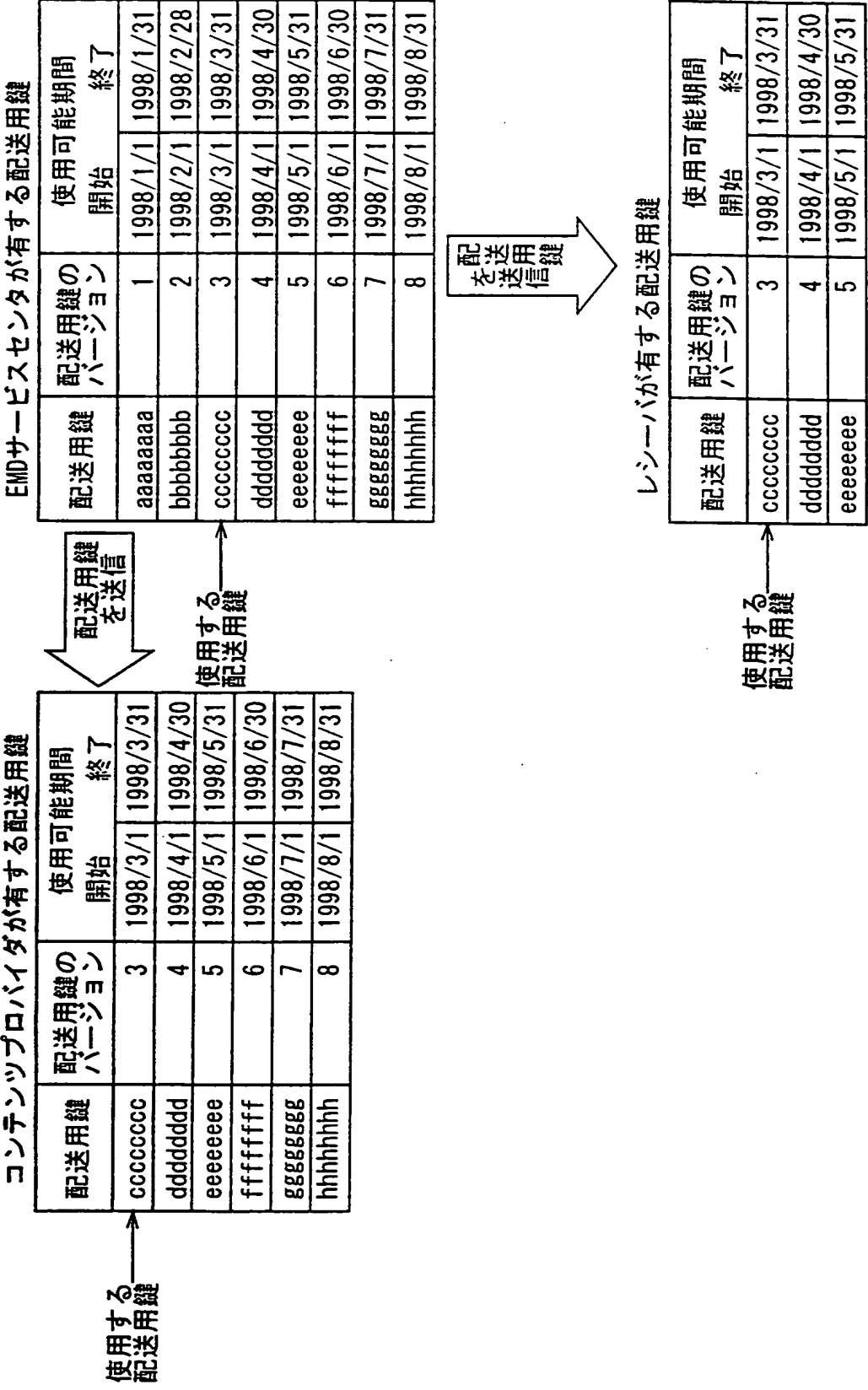


図 6

**This Page Blank (uspto)**

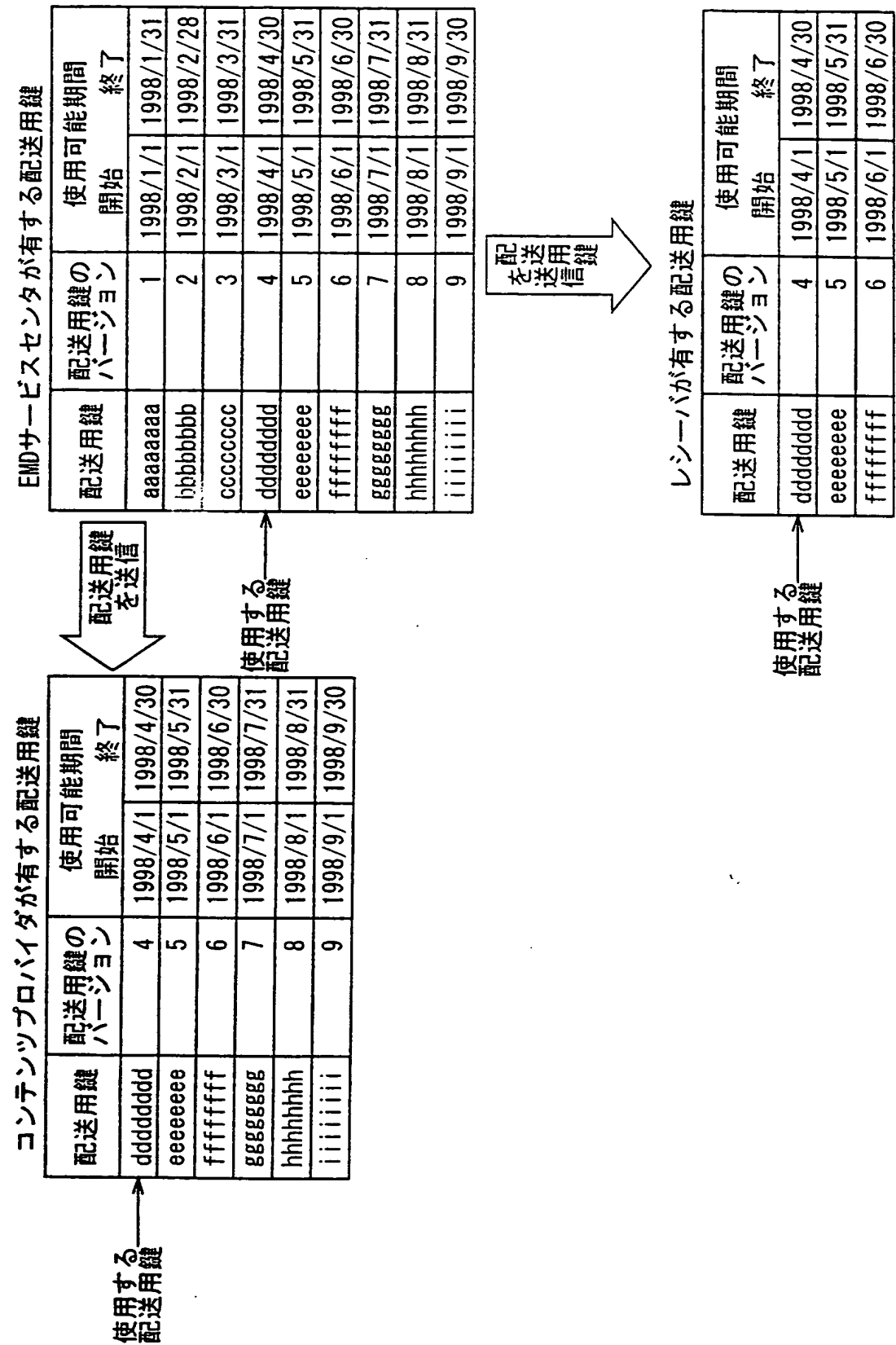


図 7

**This Page Blank (uspto)**

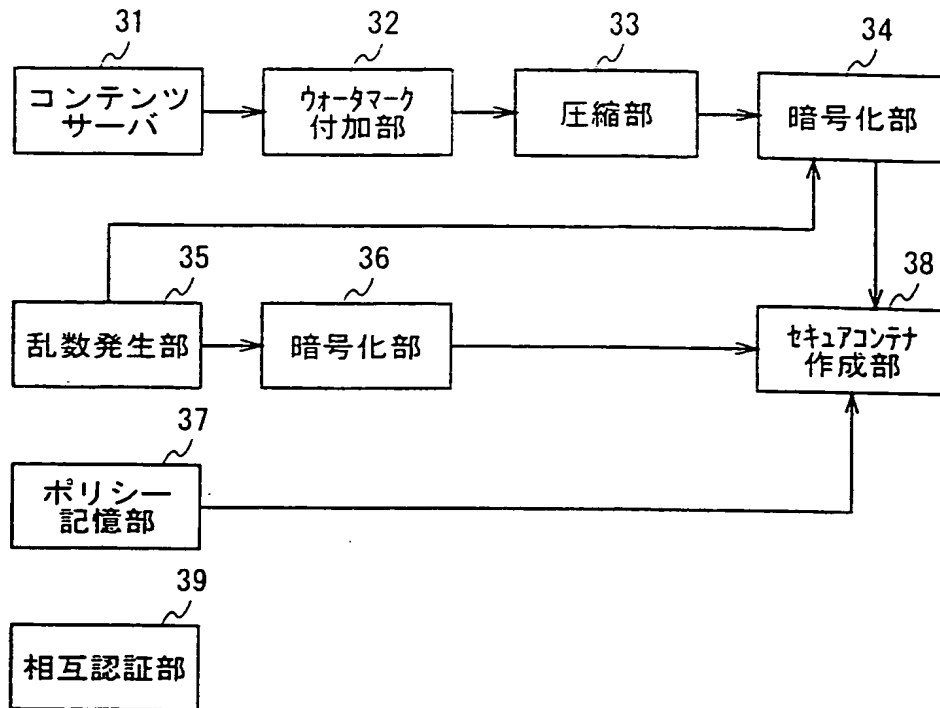
SAMのID		SAM62のID	SAM212のID	SAM311のID
機器番号		レシーバ 51の 機器番号(100番)	レシーバ 201の 機器番号(100番)	レシーバ 301の 機器番号(25番)
決済ID		ユーザFの決済ID	ユーザFの決済ID	ユーザFの決済ID
決済 ユーザ 情報	氏名	ユーザFの氏名	ユーザFの氏名	ユーザFの氏名
	住所	ユーザFの住所	ユーザFの住所	ユーザFの住所
	電話番号	ユーザFの電話番号	ユーザFの電話番号	ユーザFの電話番号
	決済機関情報	ユーザFの決済情報	ユーザFの決済情報	ユーザFの決済情報
	生年月日	ユーザFの生年月日	ユーザFの生年月日	ユーザFの生年月日
	年齢	ユーザFの年齢	ユーザFの年齢	ユーザFの年齢
	性別	ユーザFの性別	ユーザFの性別	ユーザFの性別
	ユーザのID	ユーザFのID	ユーザFのID	ユーザFのID
	パスワード	ユーザFのパスワード	ユーザFのパスワード	ユーザFのパスワード
従属 ユーザ 情報	氏名		ユーザAの氏名	ユーザAの氏名
	住所		ユーザAの住所	ユーザAの住所
	電話番号		ユーザAの電話番号	ユーザAの電話番号
	生年月日		ユーザAの生年月日	ユーザAの生年月日
	性別		ユーザAの性別	ユーザAの性別
	ユーザのID		ユーザAのID	ユーザAのID
	パスワード		ユーザAのパスワード	ユーザAのパスワード
⋮				
利用ポイント 情報		レシーバ51の利用 ポイント情報	レシーバ201の利用 ポイント情報	レシーバ301の利用 ポイント情報

システム登録情報

図 8

**This Page Blank (uspto)**





コンテンツプロバイダ 2

図 9

**This Page Blank (uspto)**

コンテンツのID	コンテンツAのID	
コンテンツプロバイダのID	コンテンツプロバイダ2のID	
UCPのID	UCPAのID	
UCPの有効期限	UCPAの有効期限	
利用条件10	ユーザ条件10	200ポイント以上
	機器条件10	条件なし
利用条件11	ID 11	利用内容11のID
	形式11	買い取り再生
	パラメータ11	× × × ×
	管理移動許可情報	可
利用内容12	ID 12	利用内容12のID
	形式12	第1世代複製
	パラメータ12	× × × ×
	管理移動許可情報	可
利用内容13	ID 13	利用内容13のID
	形式13	期間制限再生
	パラメータ13	× × × ×
	管理移動許可情報	可
利用内容14	ID 14	利用内容14のID
	形式14	Pay Per Copy N
	パラメータ14	N回
	管理移動許可情報	不可
利用内容15	ID 15	利用内容15のID
	形式15	形式13→形式11
	パラメータ	× × ×
	管理移動許可情報	可
利用内容16	ID 16	利用内容16のID
	形式16	形式11→形式11
	パラメータ	× × ×
	管理移動許可情報	可

UCPA

図 10

**This Page Blank (uspto)**

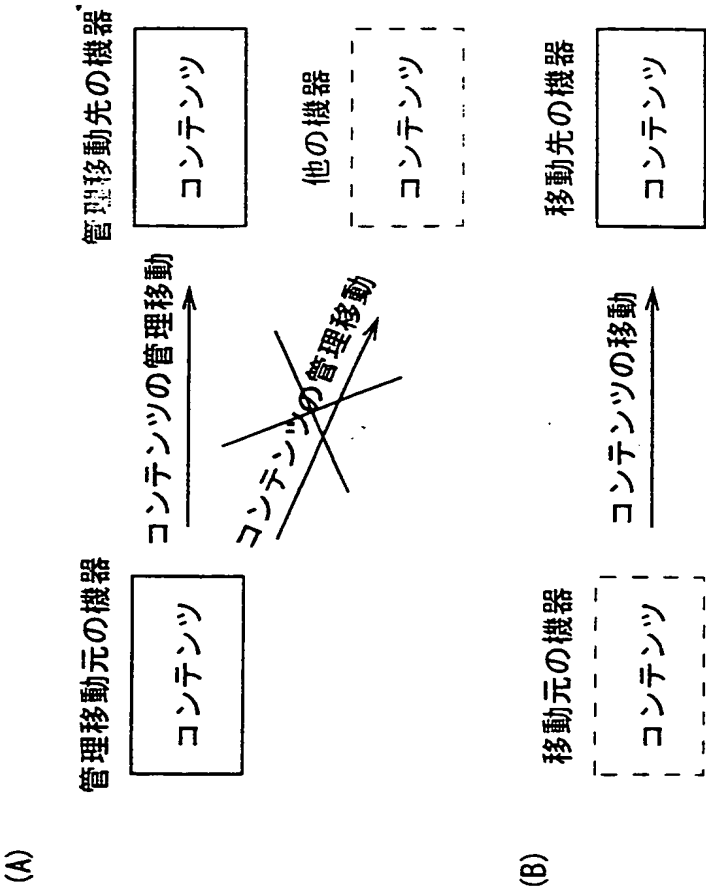


図 11

**This Page Blank (uspto)**

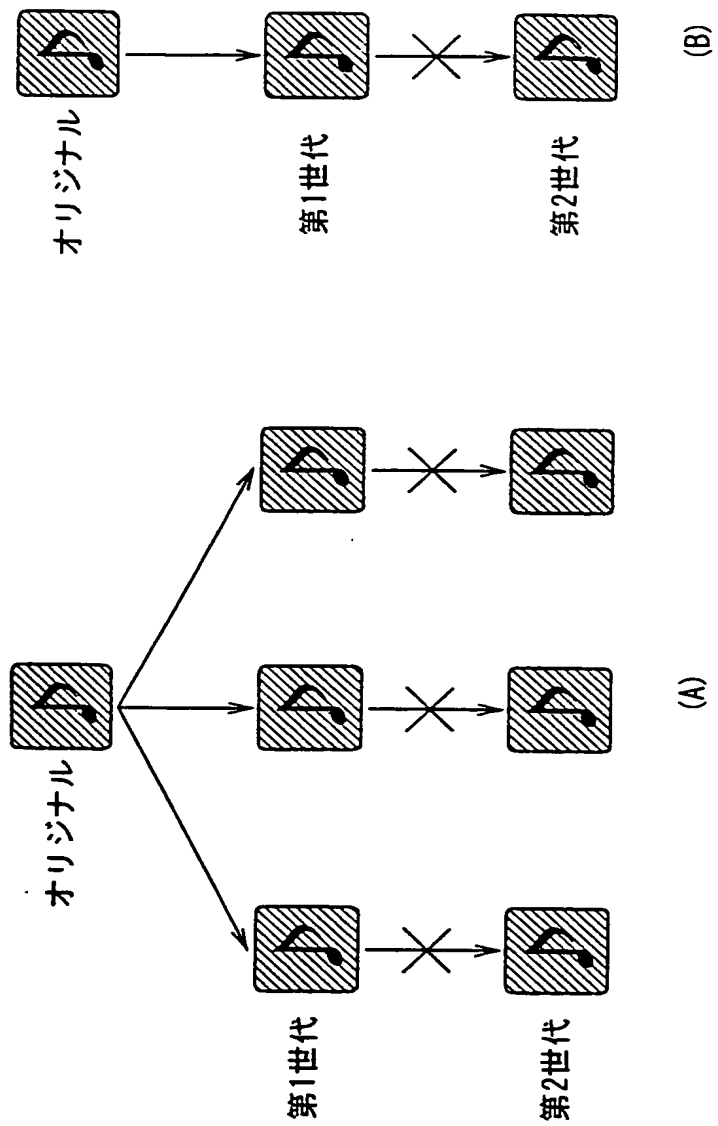


図 12

**This Page Blank (uspto)**



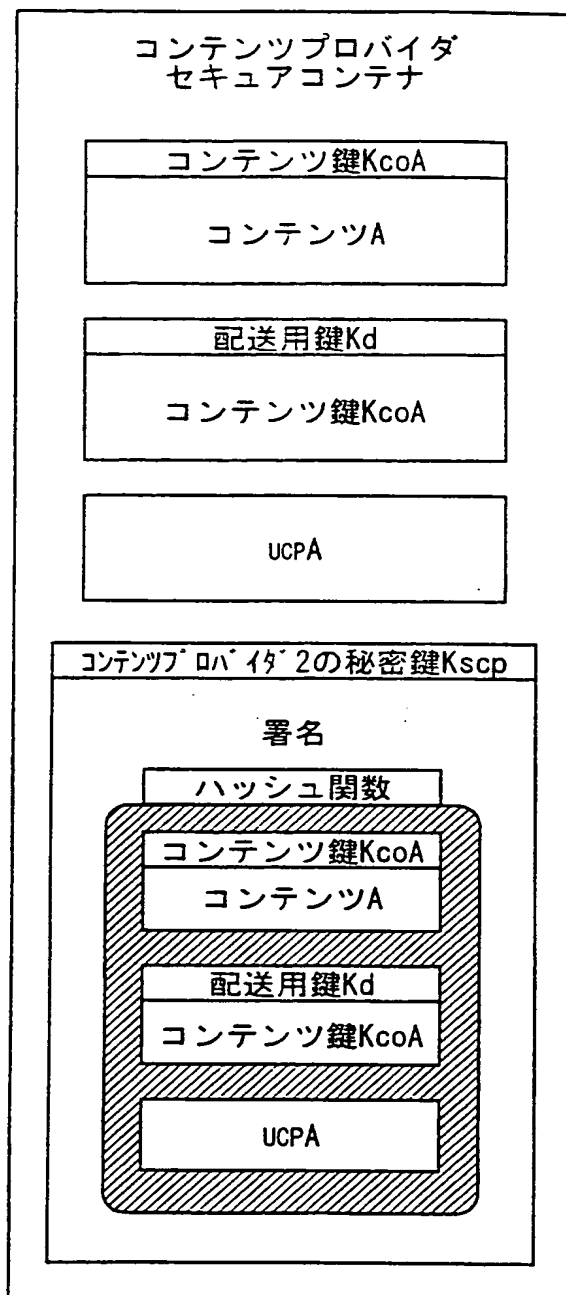


図 13

**This Page Blank (uspto)**

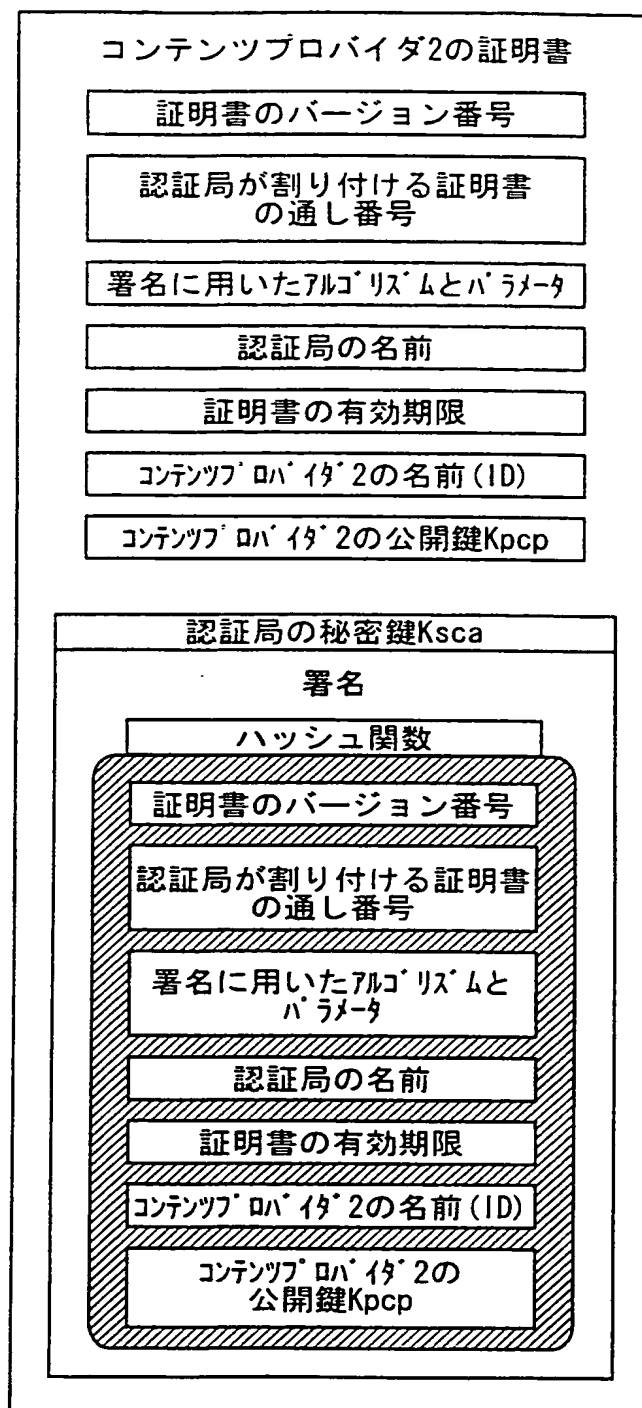
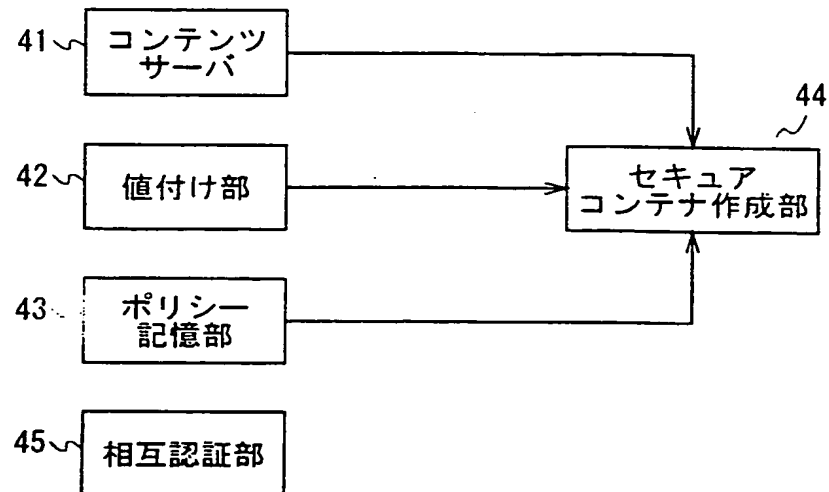


図 1 4

**This Page Blank (uspto)**



サービスプロバイダ 3

図 15

***This Page Blank (uspto)***

(A)		(B)	
コンテンツのID	コンテンツAのID	コンテンツのID	コンテンツAのID
コンテンツBのID	コンテンツBのID	コンテンツBのID	コンテンツBのID
UCPのID	UCPAのID	UCPのID	UCPAのID
サブスクリプションのID	サブスクリプションAのID	サブスクリプションのID	サブスクリプションAのID
PTのID	PTA-1のID	PTのID	PTA-2のID
PTの有効期限	PTA-1の有効期限	PTの有効期限	PTA-2の有効期限
価格条件 10	ユーザ条件 10	価格条件 20	ユーザ条件 20
	男性		女性
価格内容 11	機器条件 10	価格内容 21	機器条件 20
	条件なし		条件なし
価格内容 12	2000円	価格内容 22	1000円
価格内容 13	600円	価格内容 23	300円
価格内容 14	100円	価格内容 24	50円
価格内容 15	300円	価格内容 25	150円
価格内容 16	1950円	価格内容 26	1980円
	1000円		500円

図 16

***This Page Blank (uspto)***



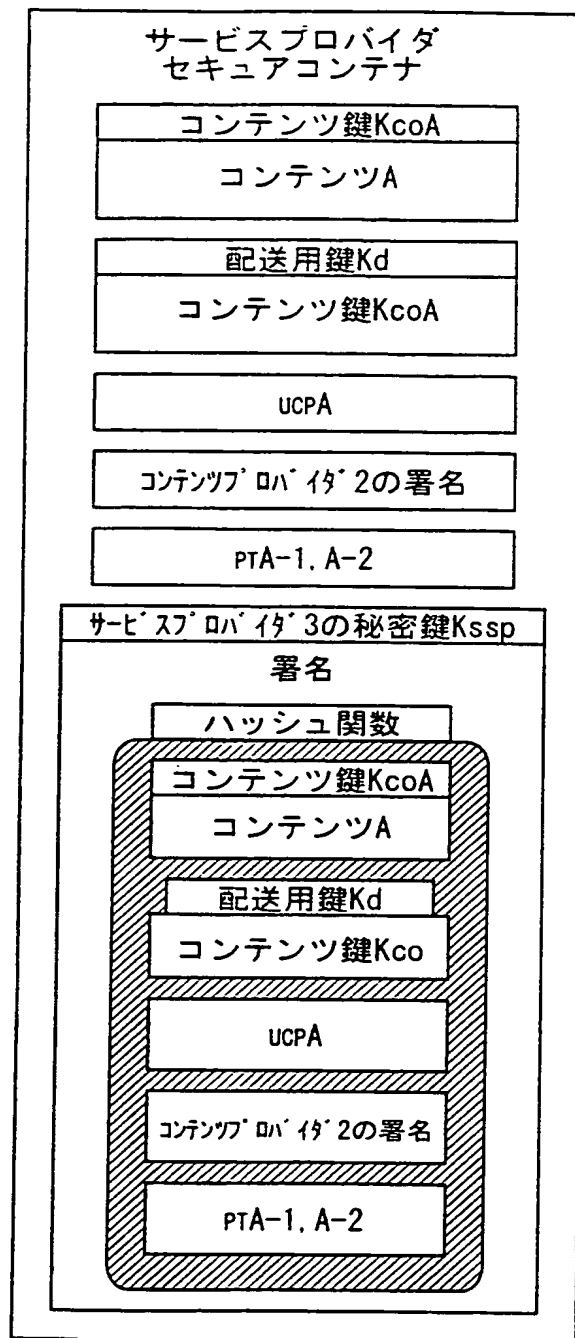


図 17

**This Page Blank (uspto)**

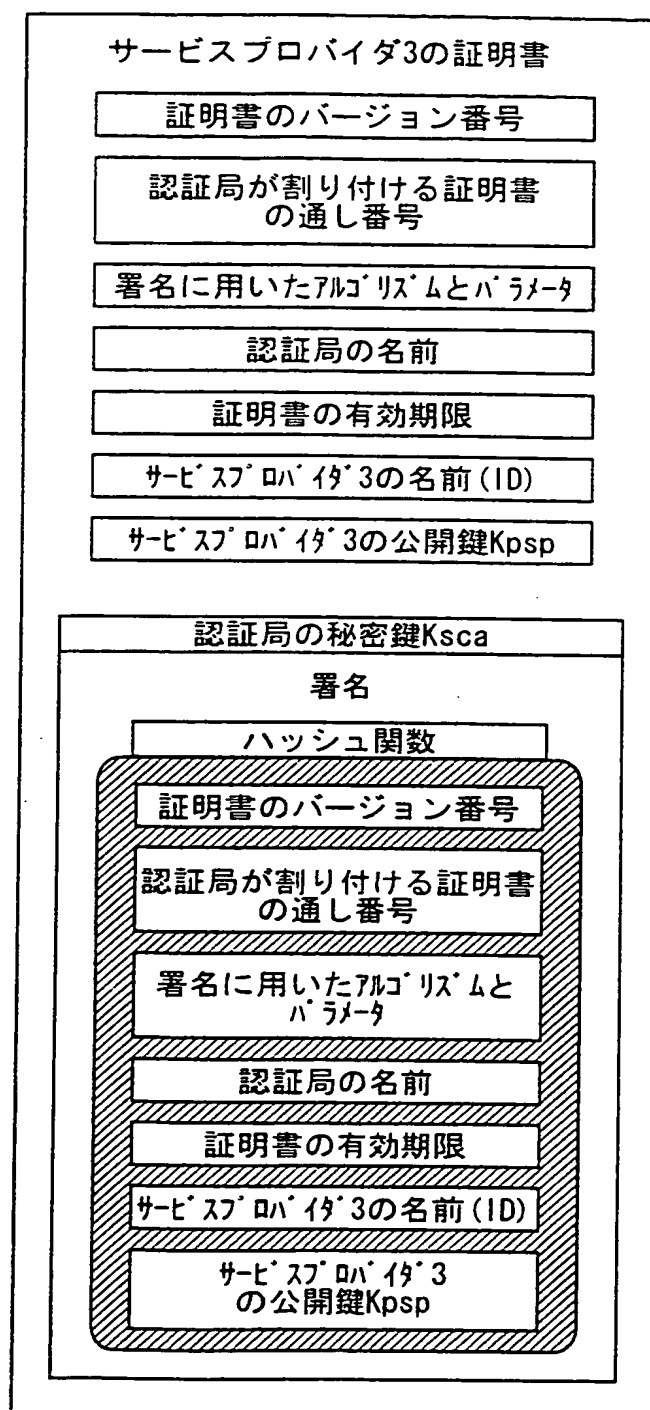


図 18

**This Page Blank (uspto)**

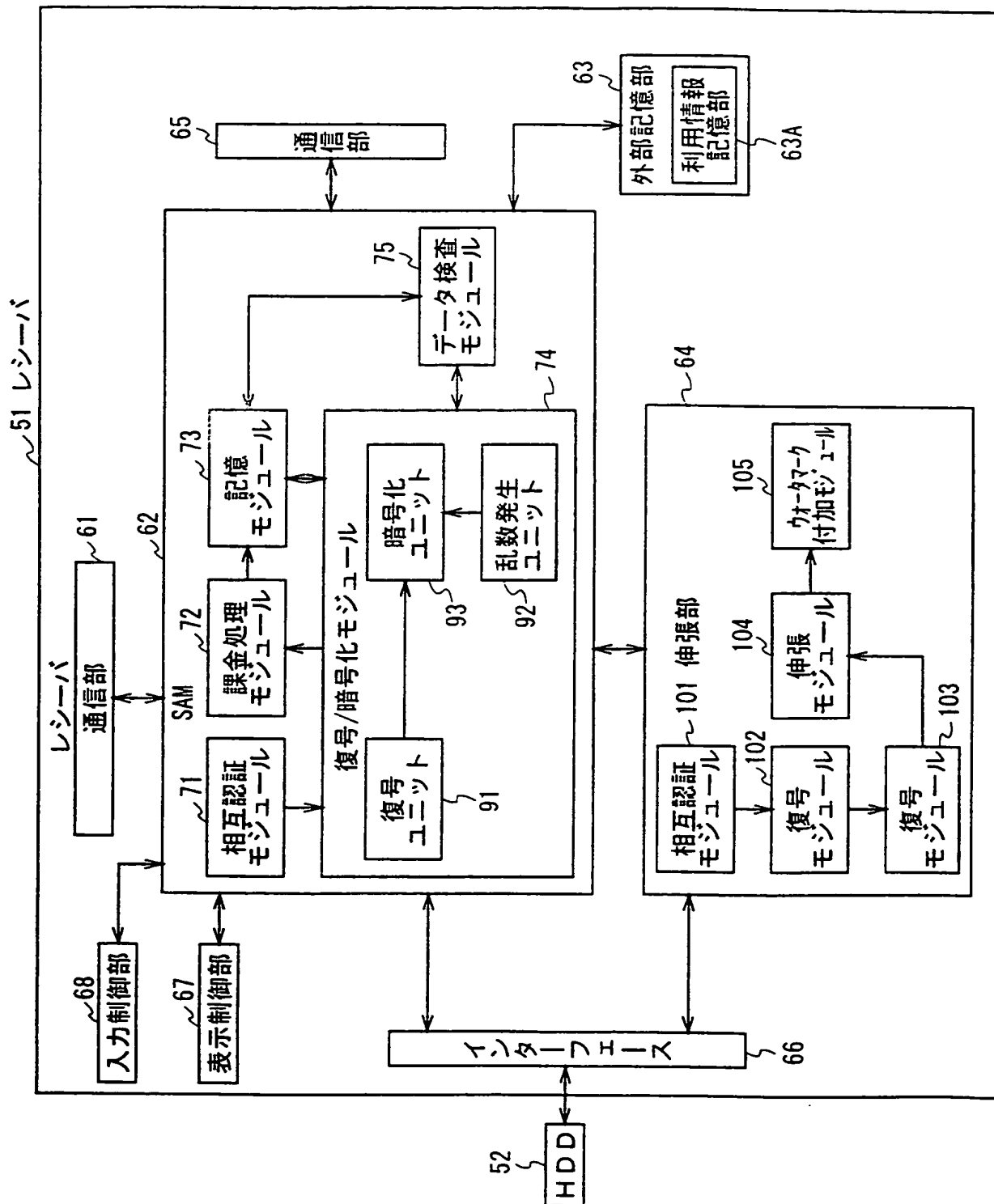


図19

**This Page Blank (uspto)**

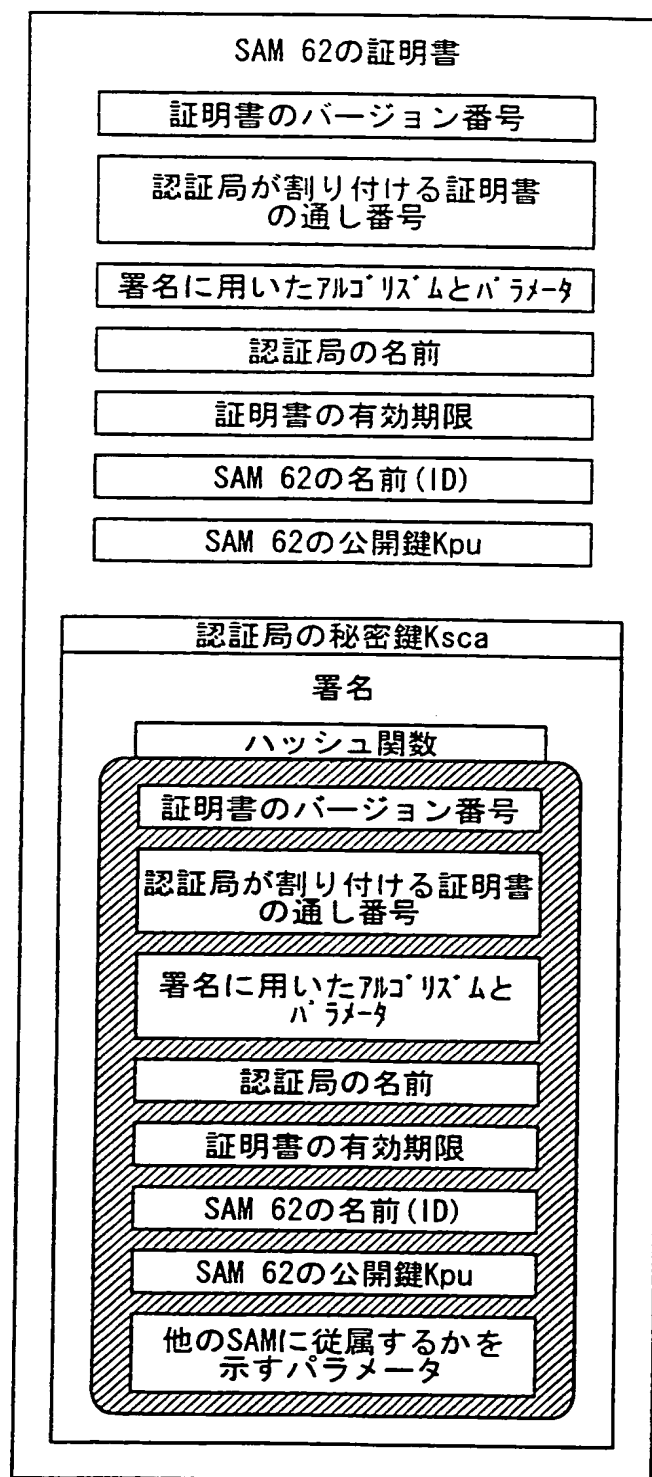


図 20

**This Page Blank (uspto)**



コンテンツのID		コンテンツAのID
コンテンツプロバイダのID		コンテンツプロバイダ2のID
UCPのID		UCPAのID
UCPの有効期限		UCPAの有効期限
サービスプロバイダのID		サービスプロバイダ3のID
PTのID		PTA-1のID
PTの有効期限		PTA-1の有効期限
UCSのID		UCSAのID
SAMのID		SAM62のID
ユーザのID		ユーザFのID
利用内容	ID	利用内容13のID
	形式	期間制限再生
	パラメータ	× × ×
	管理移動状態情報	管理移動元: SAM62のID、 管理移動先: SAM62のID
利用状態情報		× × ×

UCSA

図 2 1

**This Page Blank (uspto)**

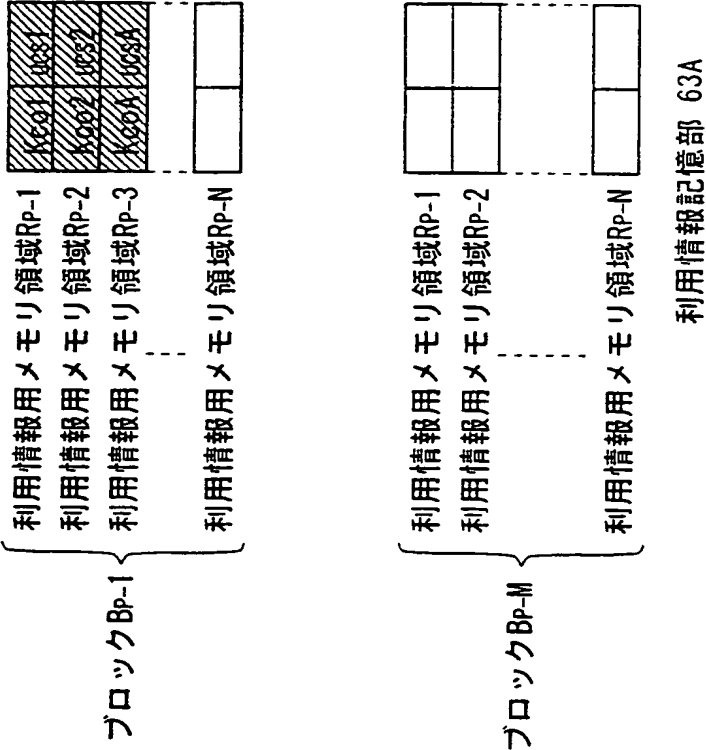


図 2 2

**This Page Blank (uspto)**

コンテンツのID		コンテンツAのID
コンテンツプロバイダのID		コンテンツプロバイダ2のID
UCPのID		UCPAのID
UCPの有効期限		UCPAの有効期限
サービスプロバイダのID		サービスプロバイダ3のID
PTのID		PTA-1のID
PTの有効期限		PTA-1の有効期限
UCSのID		UCSAのID
SAMのID		SAM62のID
ユーザのID		ユーザFのID
利用内容	ID	利用内容13のID
	形式	期間制限再生
	パラメータ	× × ×
	管理移動状態情報	管理移動元: SAM62のID、 管理移動先: SAM62のID

課金情報 A

図 2 3

**This Page Blank (uspto)**

SAM62の公開鍵Kpu		
SAM62の秘密鍵Ksu		
EMDサービスセンタ1の公開鍵Kpesc		
認証局の公開鍵Kpca		
保存用鍵Ksave		
3月分の配送用鍵Kd		
⋮		
SAM62の証明書		
基準情報 51		
課金情報		
⋮		
検査値Hp-1	検査値Hp-2	.....
.....		検査値Hp-M

図 2 4

**This Page Blank (uspto)**



SAMのID		SAM62のID	
機器番号		レシーバ 51の機器番号(100番)	
決済ID		ユーザFの決済ID	
課金の上限額		正式登録時の課金の上限額	
決済ユーザ情報	氏名	ユーザFの氏名	
	住所	ユーザFの住所	
	電話番号	ユーザFの電話番号	
	決済機関情報	ユーザFの決済機関情報	
	生年月日	ユーザFの生年月日	
	年齢	ユーザFの年齢	
	性別	ユーザFの性別	
	ユーザのID	ユーザFのID	
パスワード		ユーザFのパスワード	
従属ユーザ情報	氏名		
	住所		
	電話番号		
	生年月日		
	性別		
	ユーザのID		
	パスワード		
⋮			
利用ポイント情報		レシーバ51の利用ポイント情報	

基準情報 51

図 2 5

**This Page Blank (uspto)**

リスト部									
SAM ID	ユーザID	購入処理	課金処理	課金機器	コンデンツ供給機器	状態フラグ	登録条件署名	登録リスト署名	
ユーザー51の登録条件	ユーザー51のID	可	可	SAM62のID	なし	制限なし	××××	××××	
ユーザー201の登録条件	ユーザー201のID	可	可	SAM212のID	SAM62のID	制限なし	××××		
ユーザー301の登録条件	ユーザー301のID	不可	不可	なし	SAM62のID	制限なし	××××		

対象SAM ID

SAM62のID

有効期限

××××

バージョン番号

××××

接続されている機器数

3

対象SAM情報部

図 26

**This Page Blank (uspto)**

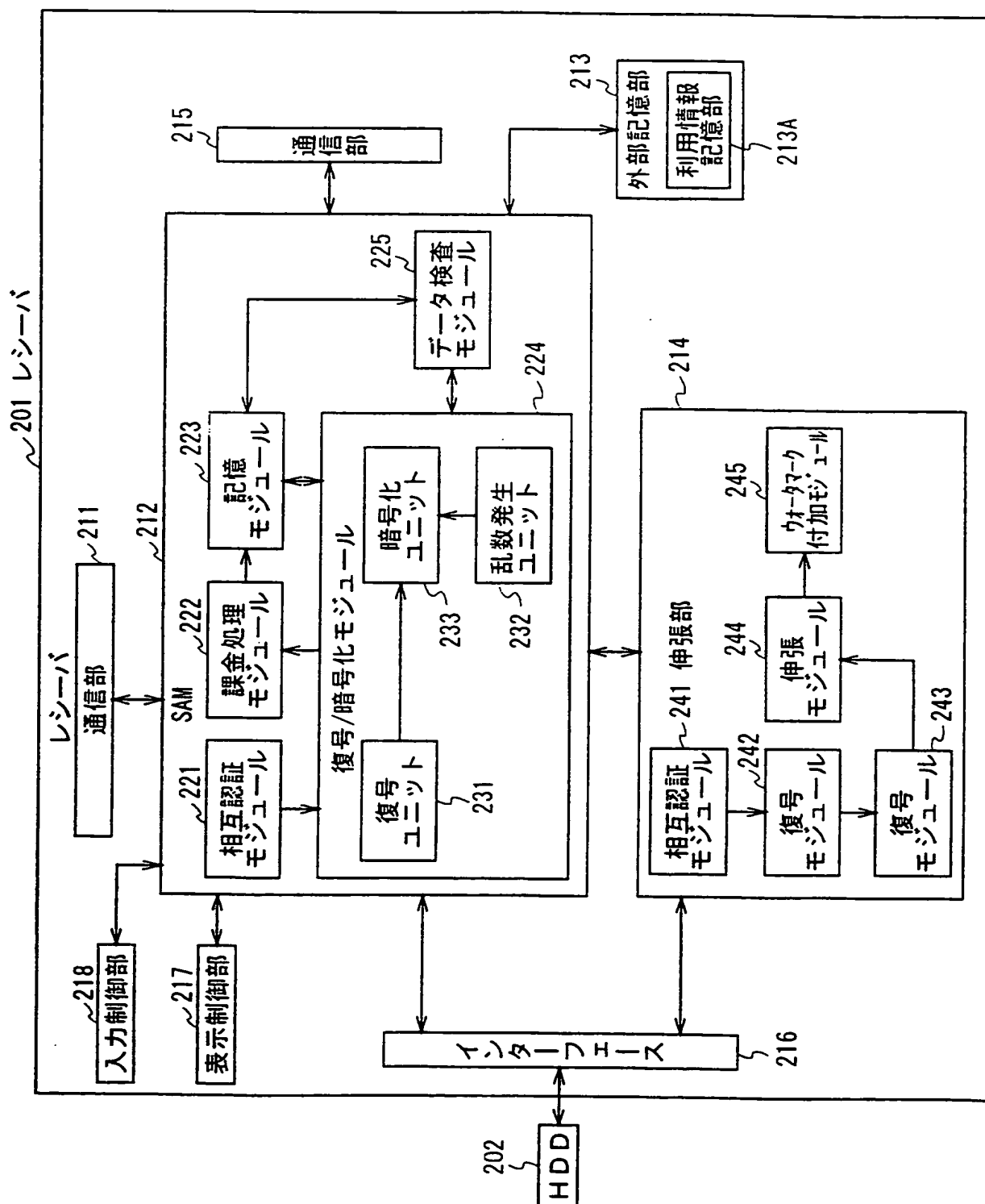


図27

**This Page Blank (uspto)**

SAMのID		SAM212のID	
機器番号		レシーバ 201の機器番号(100番)	
決済ID		ユーザFの決済ID	
課金の上限度額		正式登録時の上限度額	
決済ユーザ情報	氏名	ユーザFの氏名	
	住所	ユーザFの住所	
	電話番号	ユーザFの電話番号	
	決済機関情報	ユーザFの決済情報	
	生年月日	ユーザFの生年月日	
	年齢	ユーザFの年齢	
	性別	ユーザFの性別	
	ユーザのID	ユーザFのID	
	パスワード	ユーザFのパスワード	
従属ユーザ情報	氏名	ユーザAの氏名	
	住所	ユーザAの住所	
	電話番号	ユーザAの電話番号	
	生年月日	ユーザAの生年月日	
	性別	ユーザAの性別	
	ユーザのID	ユーザAのID	
	パスワード	ユーザAのパスワード	
利用ポイント情報		レシーバ201の利用ポイント情報	

基準情報 201

図 2 8

***This Page Blank (uspto)***



レジャー51の登録条件		リスト部						
SAM ID	ユーザID	購入処理	課金処理	課金機器	コンテンツ供給機器	状態フラグ	登録条件署名	登録リスト署名
SAM62のID	ユーザFのID	可	可	SAM62のID	なし	制限なし	××××	××××
SAM212のID	ユーザFのID	可	可	SAM212のID	SAM62のID	制限なし	××××	

対象SAM ID

SAM212のID

有効期限

××××

バージョン番号

××××

接続されている機器数

2

対象SAM情報部

図 2 9

**This Page Blank (uspto)**

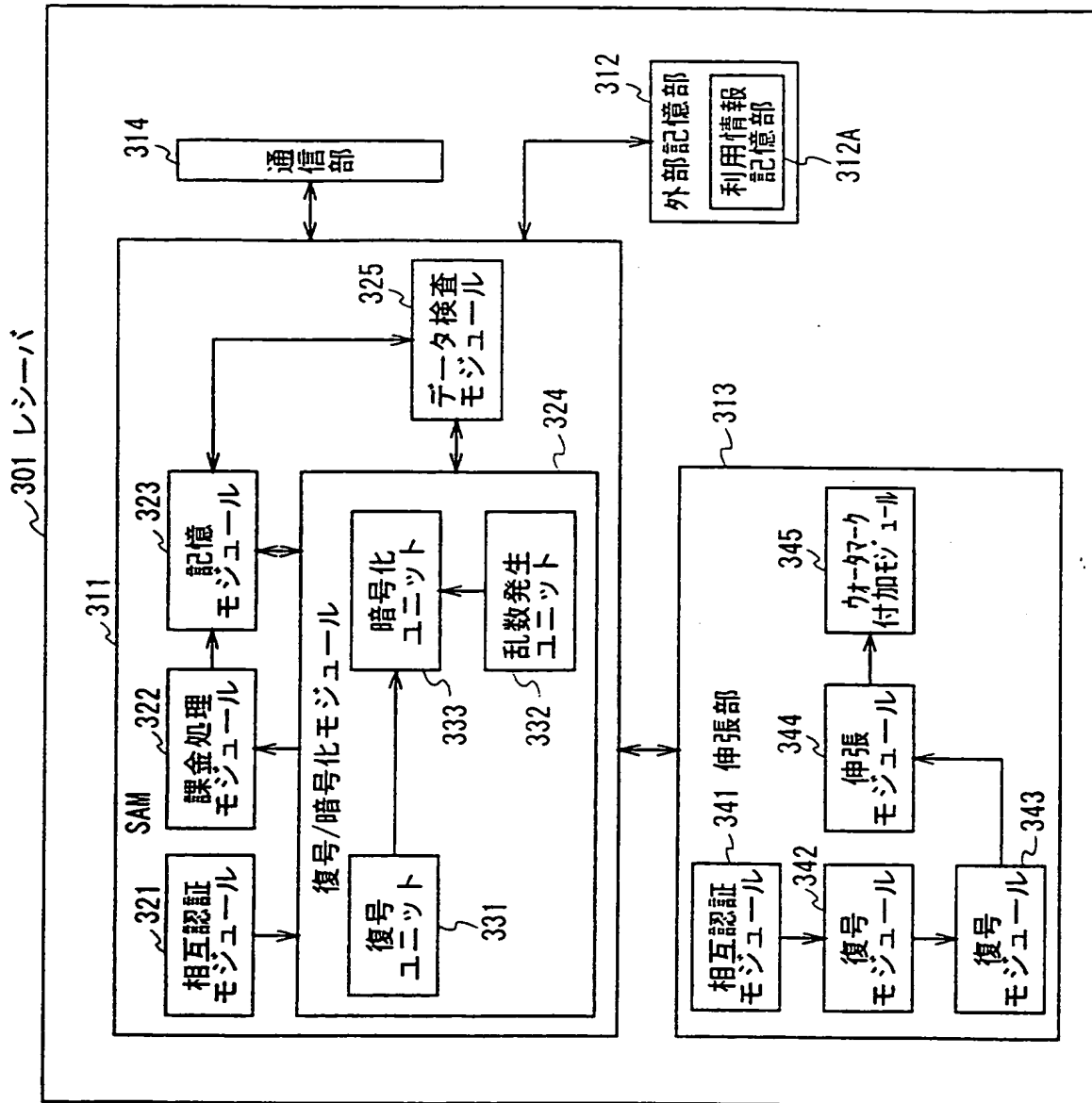


図30

**This Page Blank (uspto)**

SAMのID		SAM311のID	
機器番号		レシーバ 301の機器番号 (25番)	
決済ID		ユーザFの決済ID	
課金の上限額		正式登録時の上限額	
決済ユーザ情報	氏名	ユーザFの氏名	
	住所	ユーザFの住所	
	電話番号	ユーザFの電話番号	
	決済機関情報	ユーザFの決済情報	
	生年月日	ユーザFの生年月日	
	年齢	ユーザFの年齢	
	性別	ユーザFの性別	
	ユーザのID	ユーザFのID	
	パスワード	ユーザFのパスワード	
従属ユーザ情報	氏名	ユーザAの氏名	
	住所	ユーザAの住所	
	電話番号	ユーザAの電話番号	
	生年月日	ユーザAの生年月日	
	性別	ユーザAの性別	
	ユーザのID	ユーザAのID	
	パスワード	ユーザAのパスワード	
⋮			
利用ポイント情報		レシーバ301のポイント情報	

基準情報 301

図 3 1

**This Page Blank (uspto)**

リスト部

SAM ID	ユーザID	購入 処理	課金 処理	課金機器	コンテンツ 供給機器	状態 フラグ
SAM311のID	ユーザFのID	不可	不可	なし	SAM62のID	制限 なし

ユーザ301の  
登録条件

対象SAM ID

SAM311のID

有効期限

xxx x

パージョン番号

xxx x

接続されている機器数

2

対象SAM情報部

図 3 2

This Page Blank (uspto)

This Page Blank (uspto)



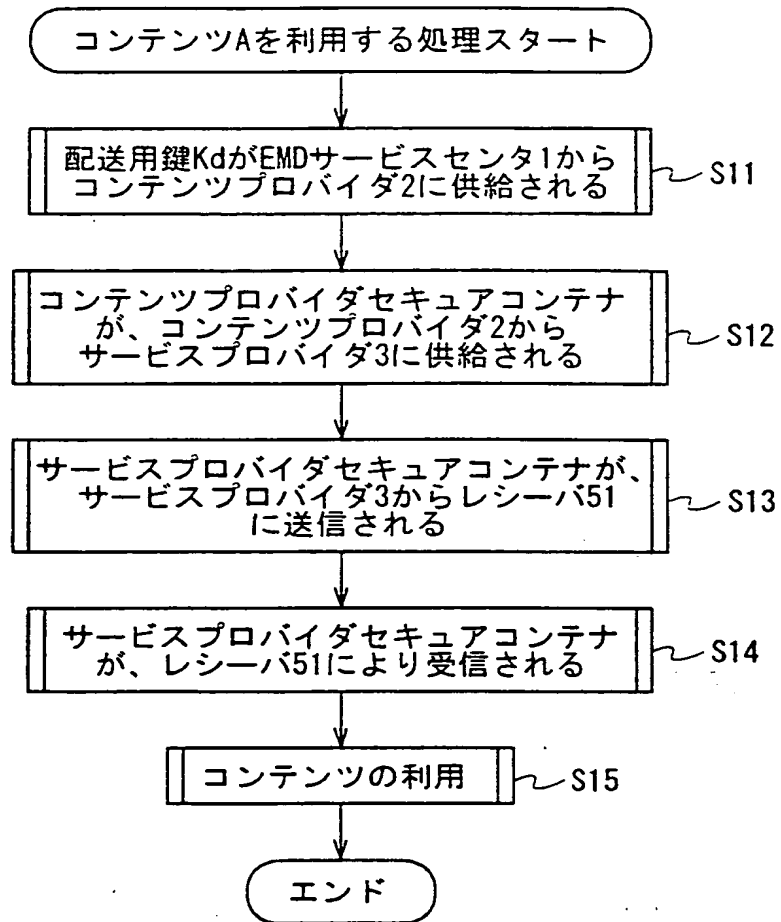


図 3 3

***This Page Blank (uspto)***

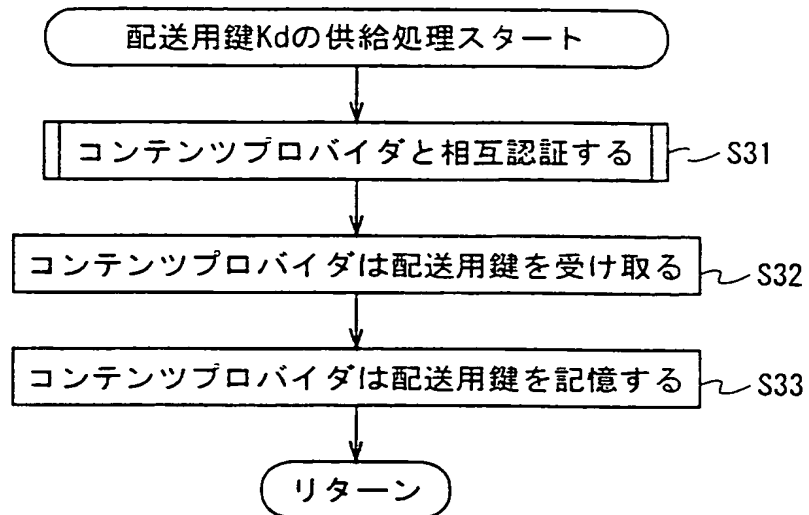


図 3 4

**This Page Blank (uspto)**

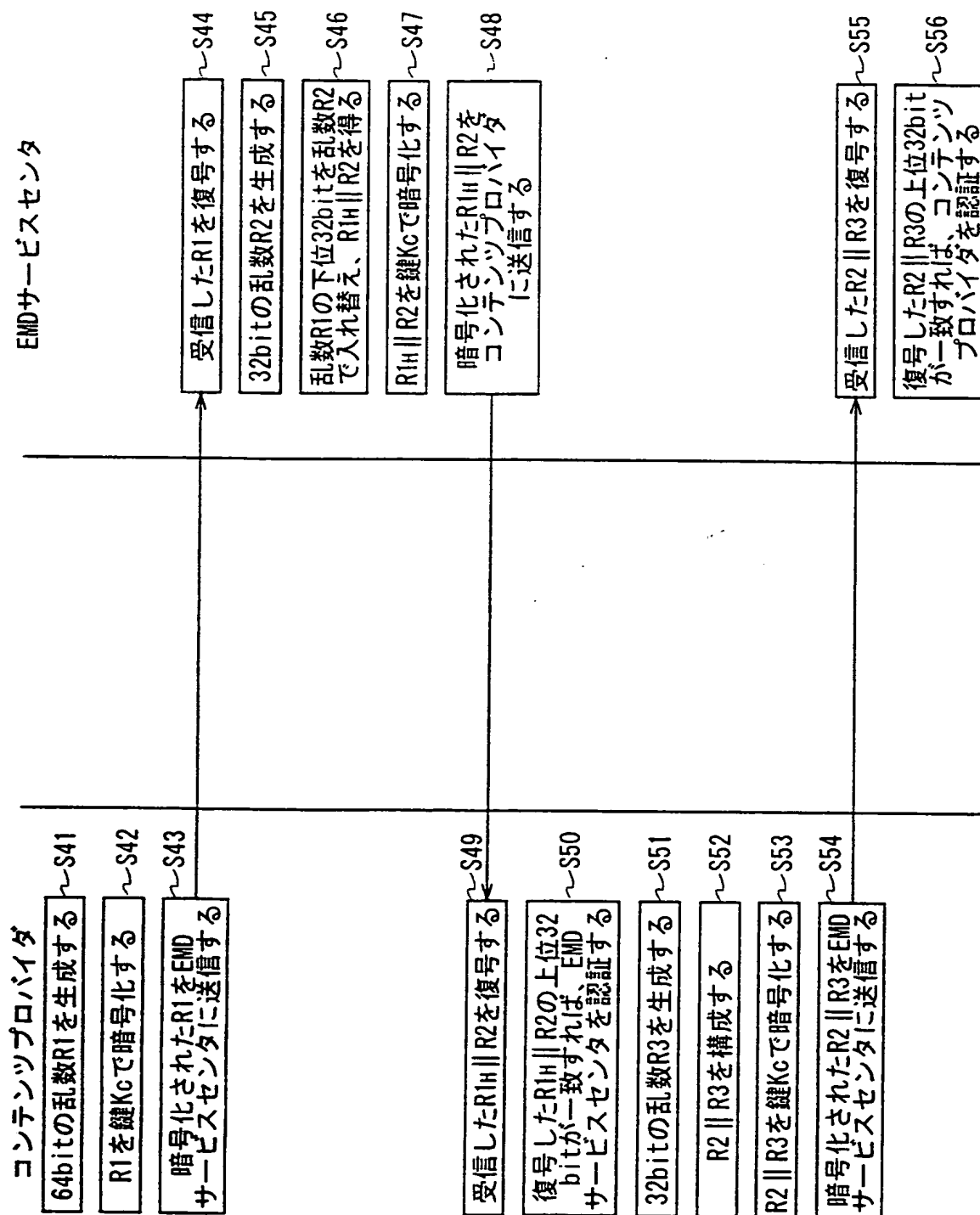


図 3 5

**This Page Blank (uspto)**

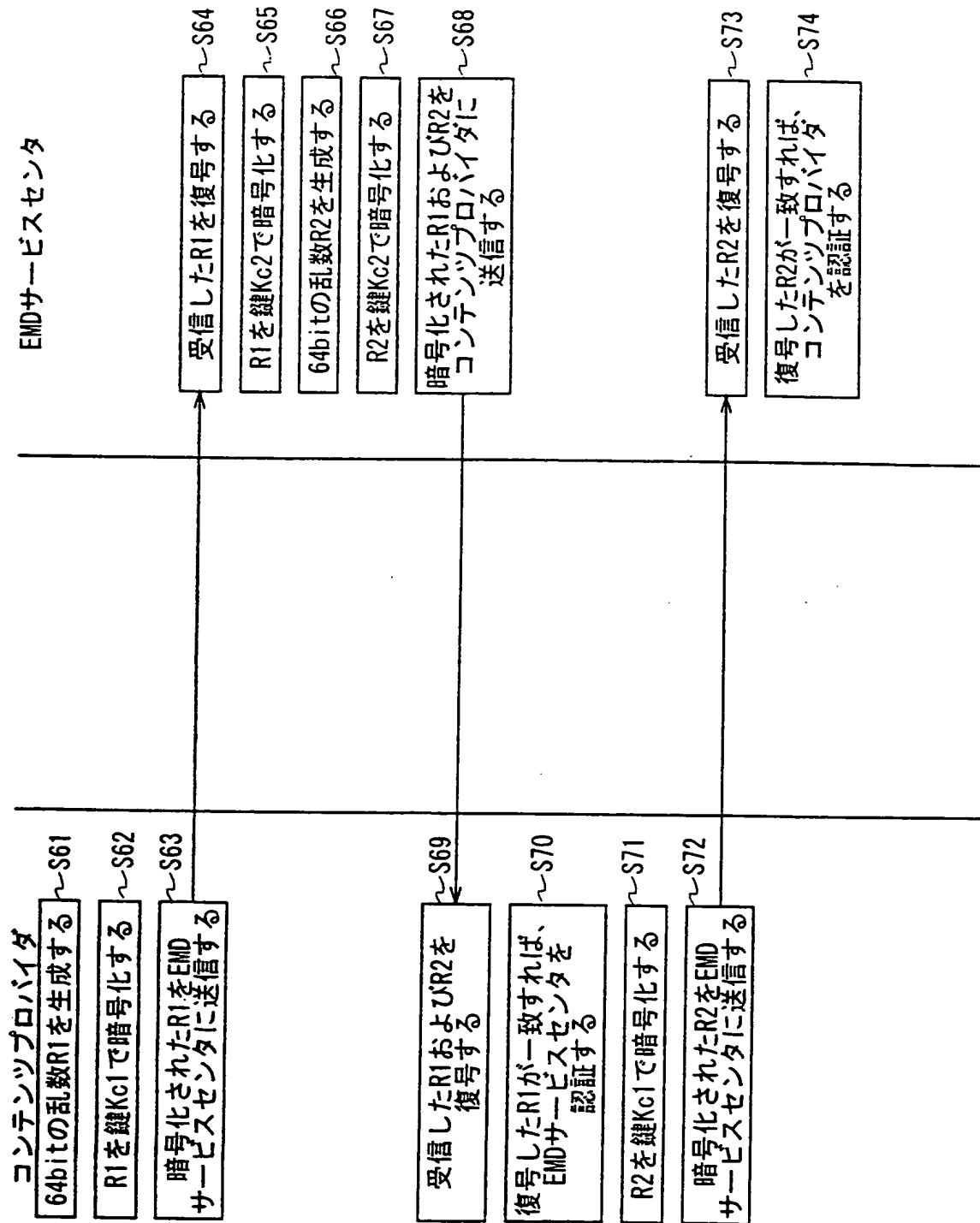


図 3 6

***This Page Blank (uspto)***



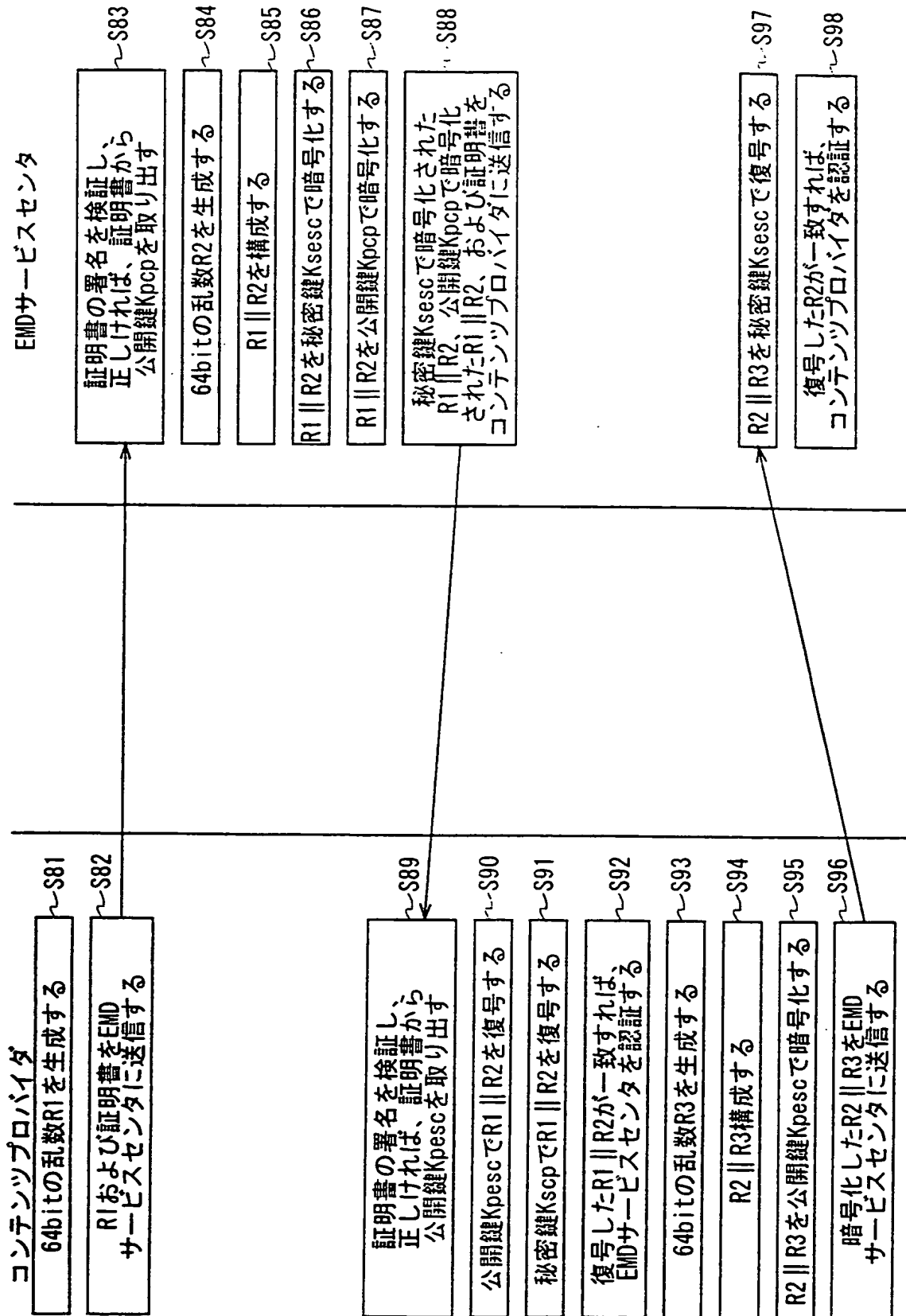


図 37

**This Page Blank (uspto)**

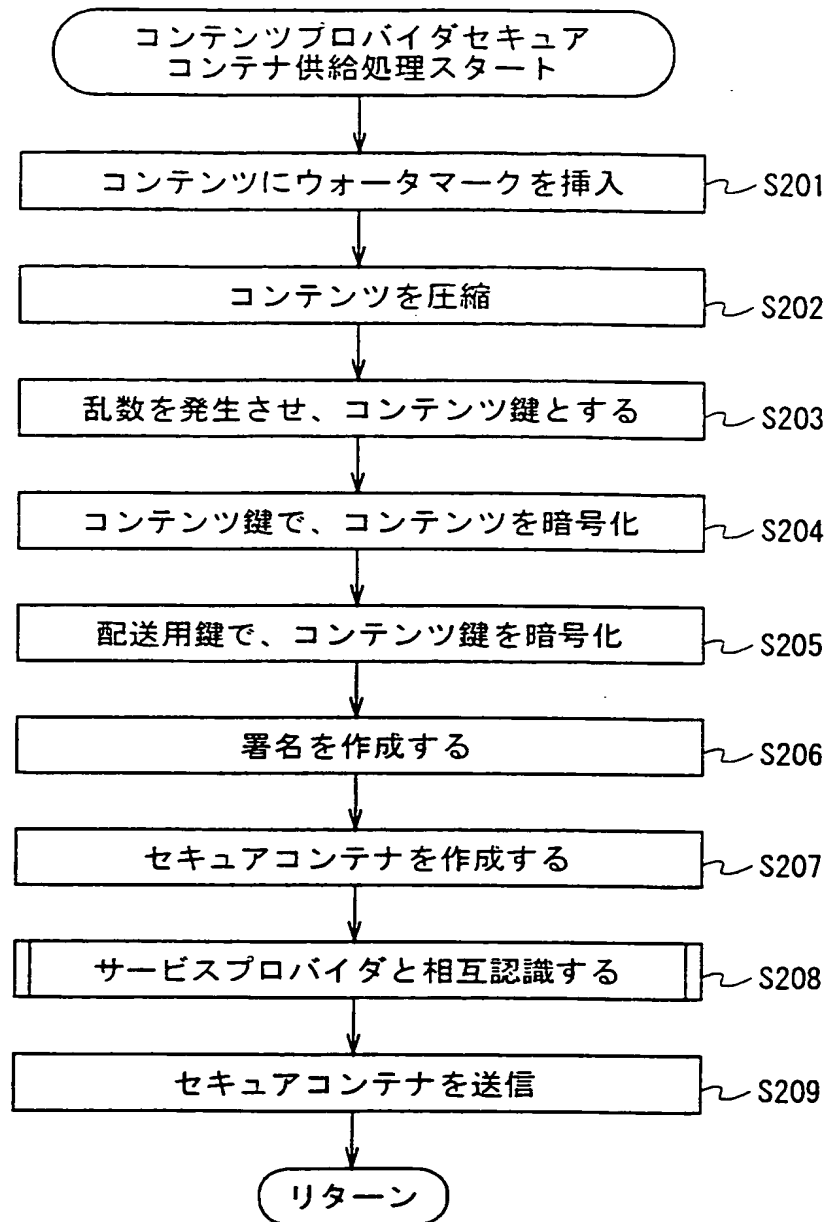


図 3 8

**This Page Blank (uspto)**

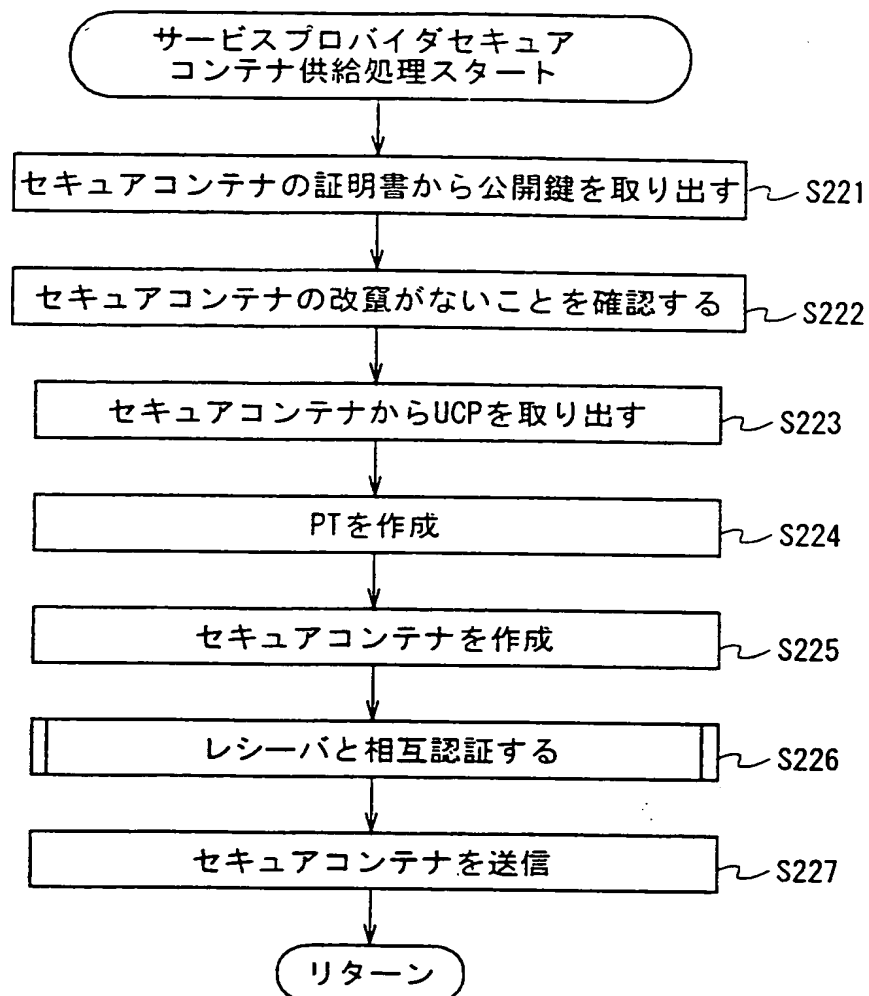


図 3 9

***This Page Blank (uspto)***

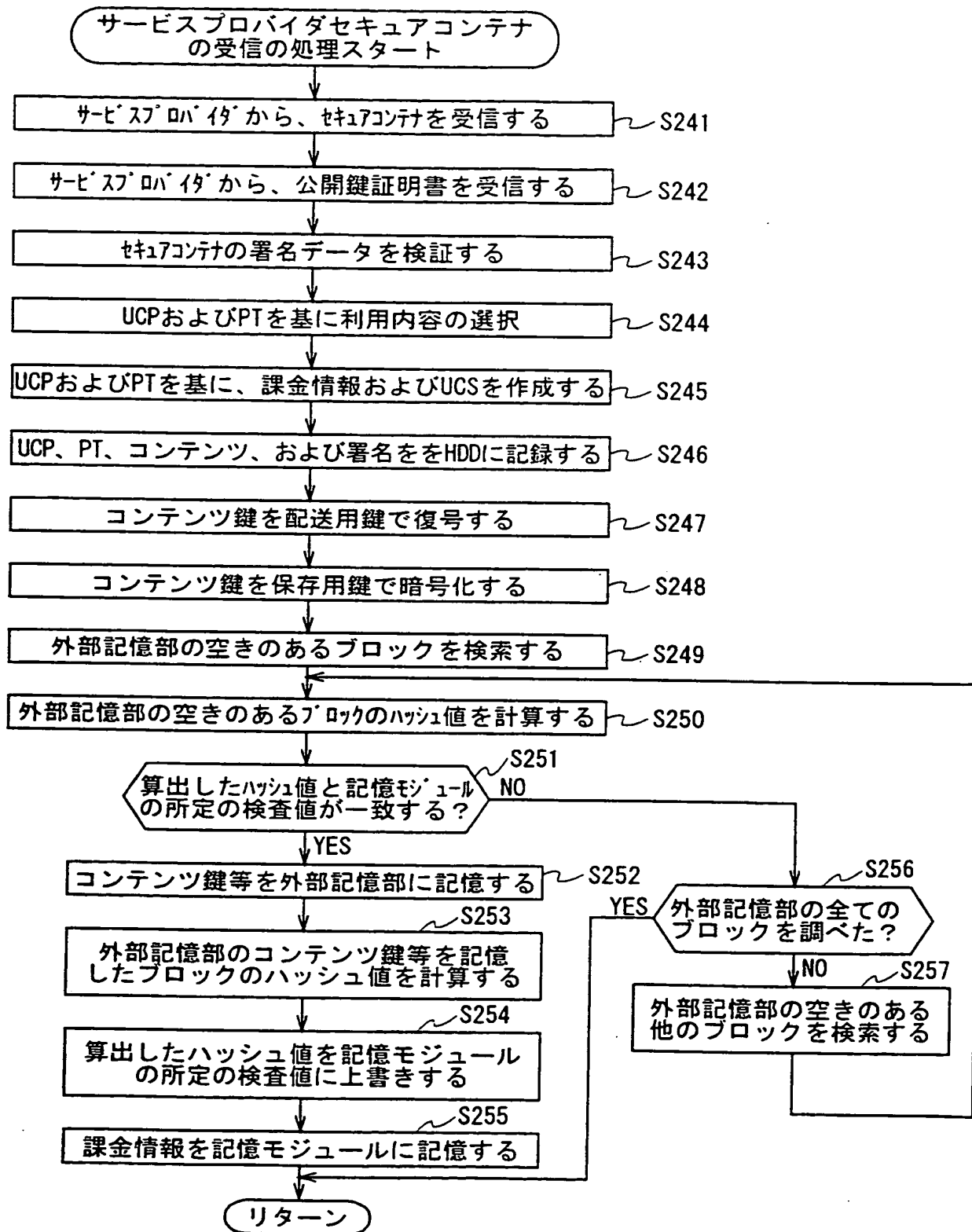


図 40

**This Page Blank (uspto)**



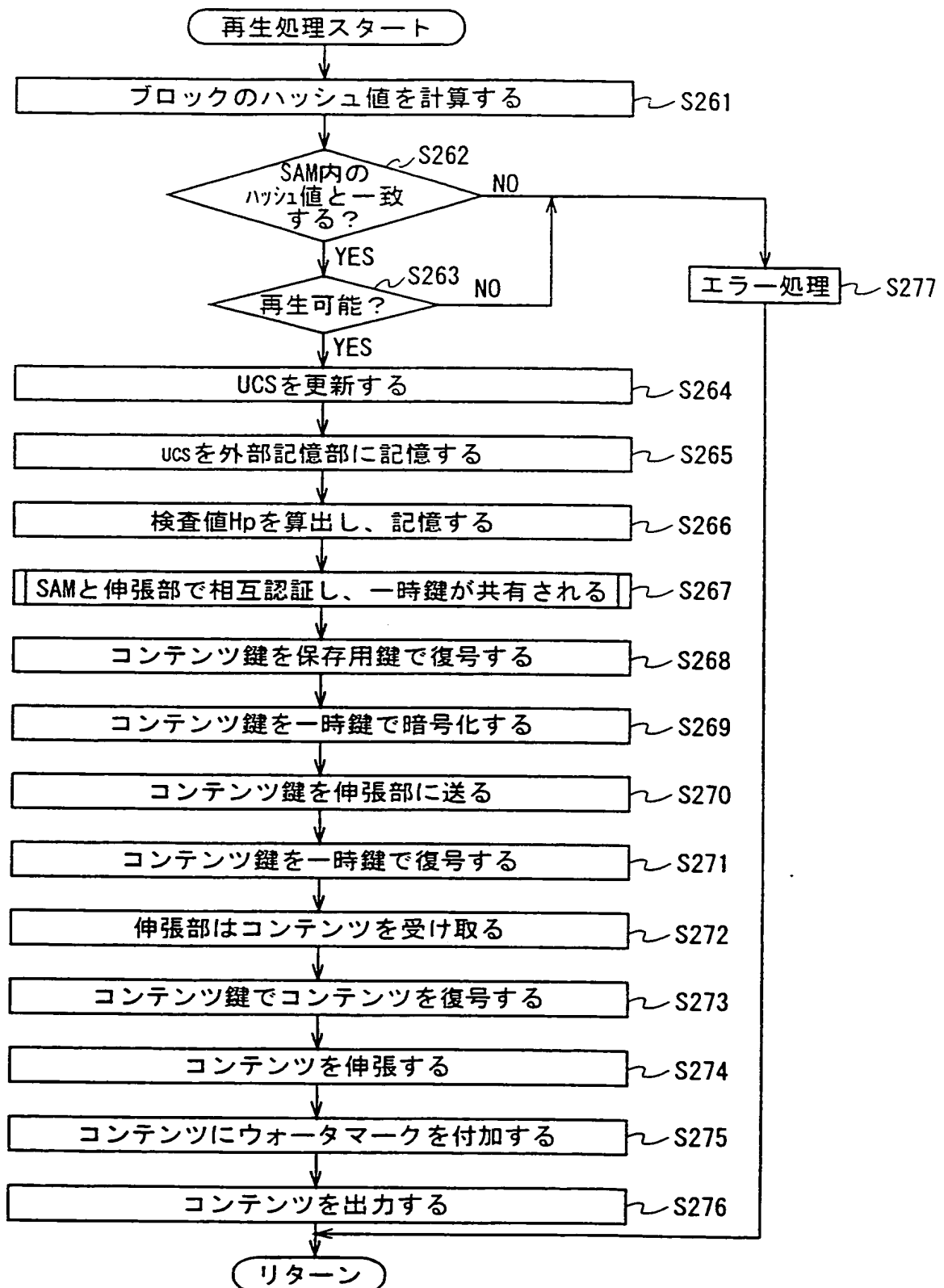


図 4 1

***This Page Blank (uspto)***

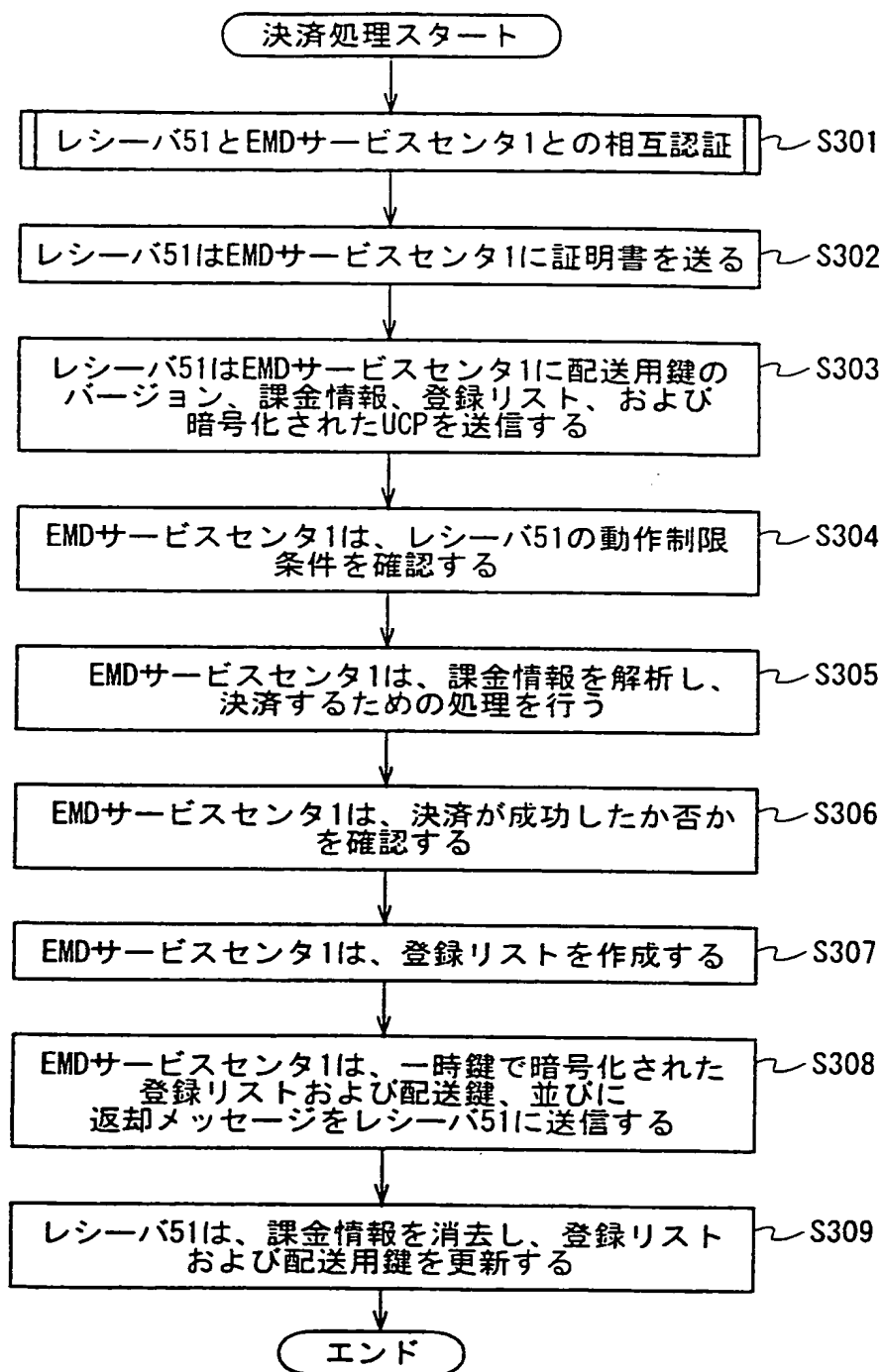


図 4 2

**This Page Blank (uspto)**

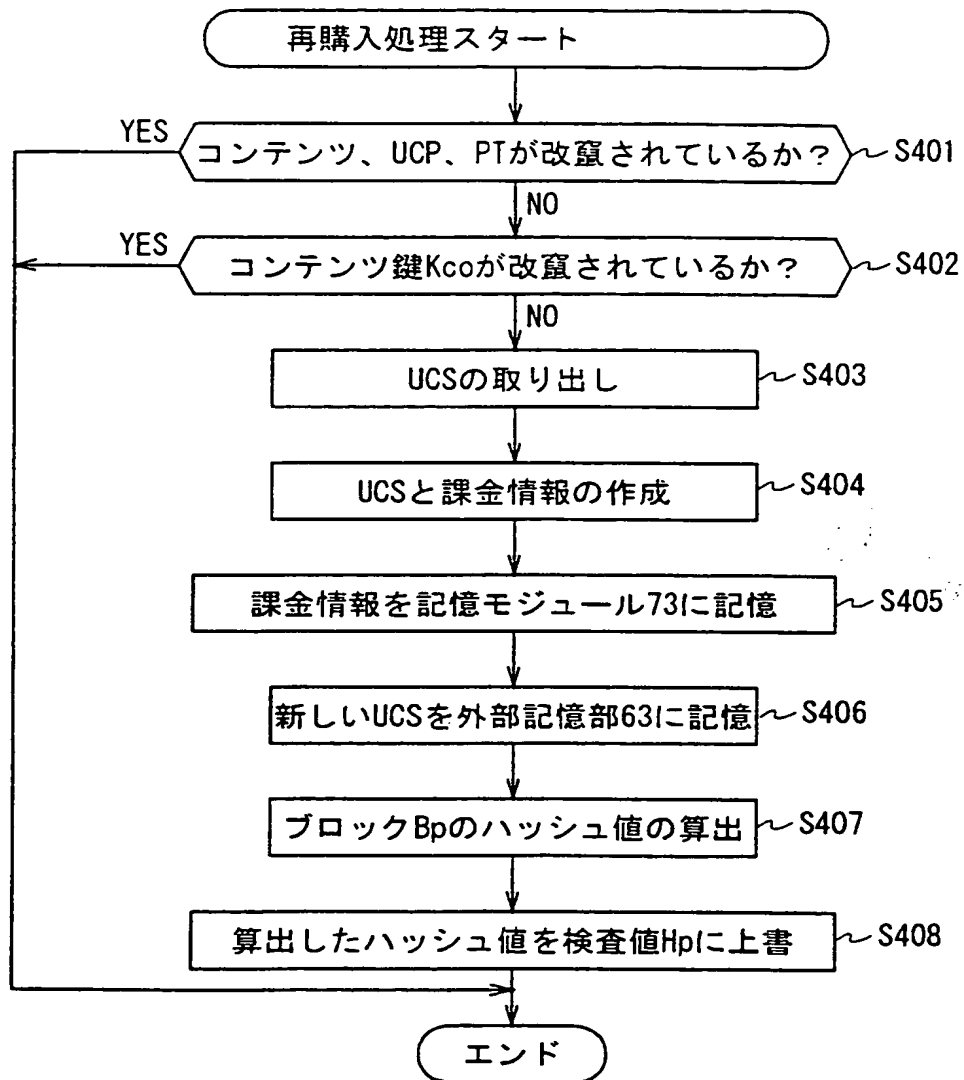


図 4 3

**This Page Blank (uspto)**

コンテンツのID		コンテンツAのID
コンテンツプロバイダのID		コンテンツプロバイダ2のID
UCPのID		UCPAのID
UCPの有効期限		UCPAの有効期限
サービスプロバイダのID		サービスプロバイダ3のID
PTのID		PTA-1のID
PTの有効期限		PTA-1の有効期限
UCSのID		ucsAのID
SAMのID		SAM62のID
ユーザのID		ユーザFのID
利用内容	ID	利用内容15のID
	形式	形式13→形式11
	パラメータ	× × ×
	管理移動状態情報	管理移動元: SAM62のID、 管理移動先: SAM62のID
利用履歴		× × ×

ucsB

図 4 4

**This Page Blank (uspto)**



コンテンツのID		コンテンツAのID
コンテンツのID		コンテンツ2のID
UCPのID		ucPAのID
UCPの有効期限		ucPAの有効期限
サービスのID		サービス3のID
PTのID		PTA-1のID
PTの有効期限		PTA-1の有効期限
UCSのID		ucsAのID
SAMのID		SAM62のID
ユーザのID		ユーザFのID
利用内容	ID	利用内容15のID
	形式	形式13→形式11
	パラメータ	× × ×
	管理移動状態情報	管理移動元: SAM62のID、 管理移動先: SAM62のID

課金情報 B

図 4 5

**This Page Blank (uspto)**

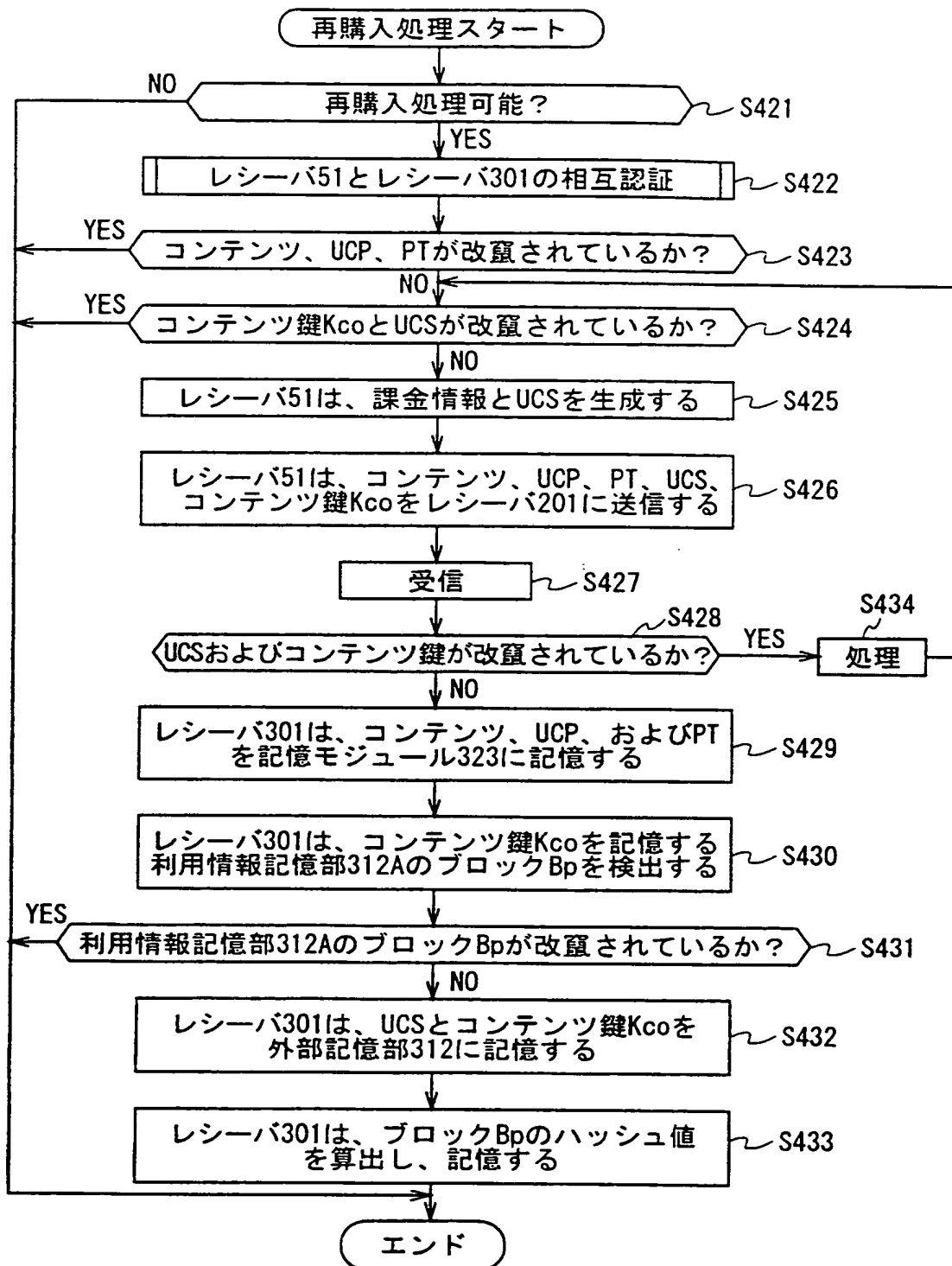


図 4 6

**This Page Blank (uspto)**

コンテンツのID		コンテンツAのID
コンテンツのID		コンテンツ2のID
UCPのID		ucPAのID
UCPの有効期限		ucPAの有効期限
サービスのID		サービス3のID
PTのID		PTA-1のID
PTの有効期限		PTA-1の有効期限
UCSのID		ucsAのID
SAMのID		SAM62のID
ユーザのID		ユーザFのID
利用内容	ID	利用内容16のID
	形式	形式11→形式11
	パラメータ	× × ×
	管理移動状態情報	管理移動元: SAM62のID、 管理移動先: SAM62のID
利用履歴		× × ×

ucsC

図 4 7

**This Page Blank (uspto)**

コンテンツのID		コンテンツAのID
コンテンツロバ イタ のID		コンテンツロバ イタ 2のID
UCPのID		UCPAのID
UCPの有効期限		UCPAの有効期限
サービスロバ イタ のID		サービスロバ イタ 3のID
PTのID		PTA-1のID
PTの有効期限		PTA-1の有効期限
UCSのID		UCSAのID
SAMのID		SAM62のID
ユーザのID		ユーザFのID
利用内容	ID	利用内容16のID
	形式	形式11→形式11
	パラメータ	× × ×
	管理移動状態情報	管理移動元: SAM62のID、 管理移動先: SAM62のID

課金情報C

図 4 8

**This Page Blank (uspto)**



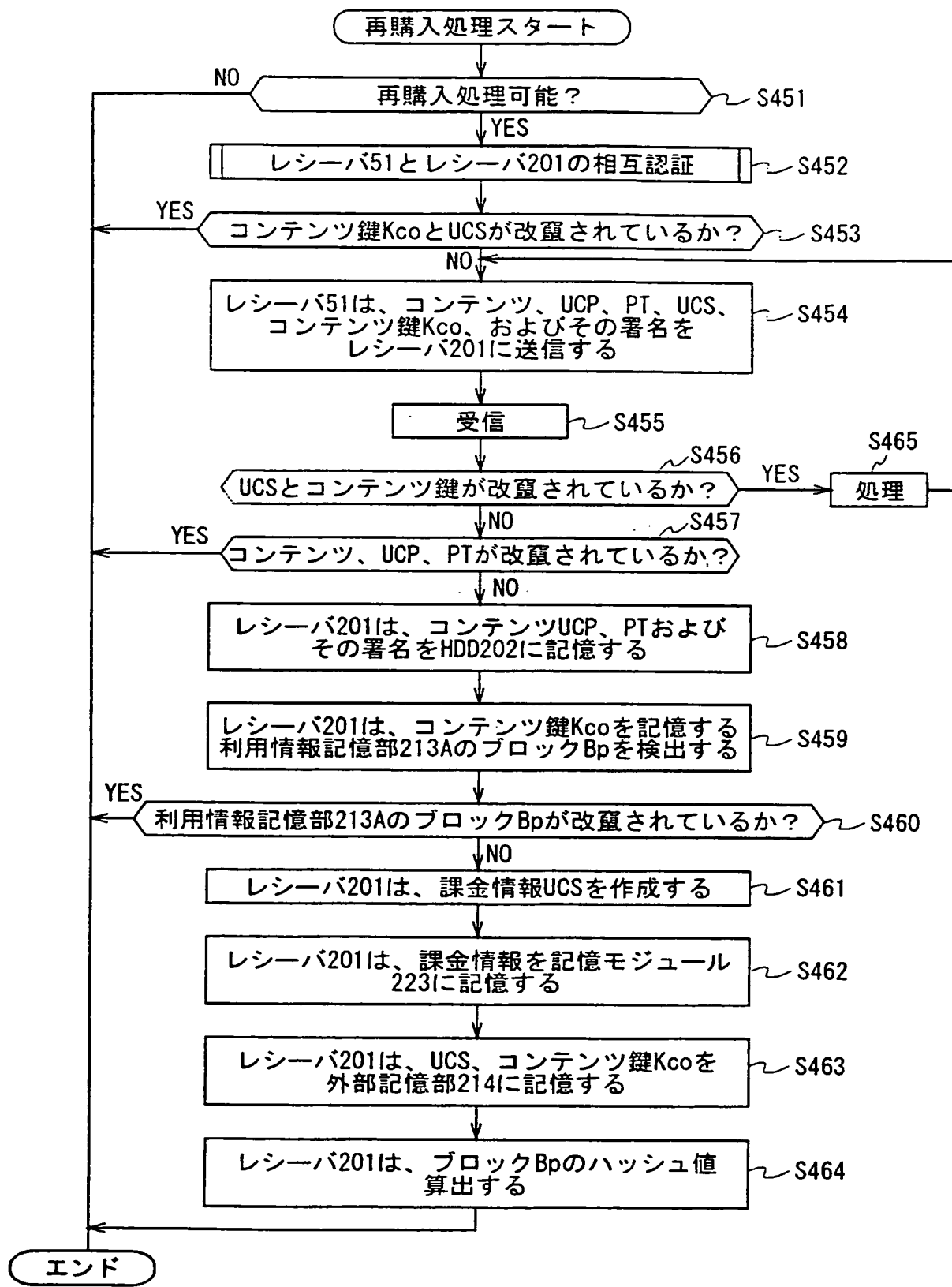


図 4 9

**This Page Blank (uspto)**

コンテンツのID		コンテンツAのID
コンテンツプロバイダのID		コンテンツプロバイダ2のID
UCPのID		ucPAのID
UCPの有効期限		ucPAの有効期限
サービスプロバイダのID		サービスプロバイダ3のID
PTのID		PTA-1のID
PTの有効期限		PTA-1の有効期限
UCSのID		ucsAのID
SAMのID		SAM212のID
ユーザのID		ユーザFのID
利用内容	ID	利用内容16のID
	形式	形式11→形式11
	パラメータ	× × ×
	管理移動状態情報	管理移動元: SAM62のID、 管理移動先: SAM62のID
利用履歴		× × ×

ucSD

図 5 0

**This Page Blank (uspto)**

***This Page Blank (uspto)***

コンテンツのID		コンテンツAのID
コンテンツプロバイダのID		コンテンツプロバイダ2のID
UCPのID		ucPAのID
UCPの有効期限		ucPAの有効期限
サービスプロバイダのID		サービスプロバイダ3のID
PTのID		PTA-1のID
PTの有効期限		PTA-1の有効期限
UCSのID		ucSAのID
SAMのID		SAM212のID
ユーザのID		ユーザFのID
利用内容	ID	利用内容16のID
	形式	形式11→形式11
	パラメータ	× × ×
	管理移動状態情報	管理移動元: SAM62のID、 管理移動先: SAM62のID

課金情報D

図 5 1

***This Page Blank (uspto)***

## 符 号 の 説 明

1 …… EMD サービスセンタ, 2 …… コンテンツプロバイダ, 3 …… サービスプロバイダ, 5 …… ユーザホームネットワーク, 11 …… サービスプロバイダ管理部, 12 …… コンテンツプロバイダ管理部, 13 …… 著作権管理部, 14 …… 鍵サーバ, 15 …… 経歴データ管理部, 16 …… 利益分配部, 17 …… 相互認証部, 18 …… ユーザ管理部, 19 …… 課金請求部, 20 …… 出納部, 21 …… 監査部, 31 …… コンテンツサーバ, 32 …… ウォータマーク付加部, 33 …… 圧縮部, 34 …… 暗号化部, 35 …… 乱数発生部, 36 …… 暗号化部, 37 …… ポリシー記憶部, 38 …… セキュアコンテナ作成部, 39 …… 相互認証部, 41 …… コンテンツサーバ, 42 …… 値付け部, 43 …… ポリシー記憶部, 44 …… セキュアコンテナ作成部, 45 …… 相互認証部, 51 …… レシーバ, 52 …… HDD, 61 …… 通信部, 62 …… SAM, 63 …… 外部記憶部, 64 …… 伸張部, 65 …… 通信部, 66 …… インタフェース, 67 …… 表示制御部, 68 …… 入力制御部, 71 …… 相互認証モジュール, 72 …… 課金処理モジュール, 73 …… 記憶モジュール, 74 …… 復号/暗号化モジュール, 75 …… データ検査モジュール, 91 …… 復号ユニット, 92 …… 乱数発生ユニット, 93 …… 暗号化ユニット, 101 …… 相互認証モジュール, 102 …… 復号モジュール, 103 …… 復号モジュール, 104 …… 伸張モジュール, 105 …… ウォータマーク付加モジュール, 201 …… レシーバ, 202 …… HDD, 211 …… 通信部, 212 …… SAM, 213 …… 外部記憶部, 214 …… 伸張部, 215 …… 通信部, 216 …… インタフェース, 217 …… 表示制御部, 218 …… 入力制御部, 221 …… 相互認証モジュール,

**This Page Blank (uspto)**



2 2 2 ……課金処理モジュール, 2 2 3 ……記憶モジュール, 2 2 4 ……復号／暗号化モジュール, 2 2 5 ……データ検査モジュール, 2 3 1 ……復号ユニット, 2 3 2 ……乱数発生ユニット, 2 3 3 ……暗号化ユニット, 2 4 1 ……相互認証モジュール, 2 4 2 ……復号モジュール, 2 4 3 ……復号モジュール, 2 4 4 ……伸張モジュール, 2 4 5 ……ウォータマーク付加モジュール

**This Page Blank (uspto)**

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP00/02288

A. CLASSIFICATION OF SUBJECT MATTER  
Int.Cl.<sup>7</sup> G06F17/60

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)  
Int.Cl.<sup>7</sup> G06F17/60

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched  
Jitsuyo Shinan Koho 1926-1996 Jitsuyo Shinan Toroku Koho 1996-2000  
Kokai Jitsuyo Shinan Koho 1971-2000 Toroku Jitsuyo Shinan Koho 1994-2000

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)  
JICST File (JOIS)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO, 96/27155, A2 (InterTrust Technologies Corp.), 06 September, 1996 (06.09.96) & JP, 10-512074, A	1-15
Y	US, 6002771, A (Sun Microsystems, Incorporated), 22 May, 1996 (22.05.96) & JP, 10-055383, A	1-15

☐ Further documents are listed in the continuation of Box C.☐ See patent family annex.

\* Special categories of cited documents:  
"A" document defining the general state of the art which is not considered to be of particular relevance  
"E" earlier document but published on or after the international filing date  
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)  
"O" document referring to an oral disclosure, use, exhibition or other means  
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention  
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone  
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art  
"&" document member of the same patent family

Date of the actual completion of the international search  
19 May, 2000 (19.05.00)

Date of mailing of the international search report  
13 June, 2000 (13.06.00)

Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

**This Page Blank (uspto)**

## 国際調査報告

国際出願番号 PCT/JPO0/02288

## A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl<sup>1</sup> G06F17/60

## B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl<sup>1</sup> G06F17/60 G06F13/00 G09C1/00 H04L9/08 G06F15/00 H04L9/32

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1926-1996年  
日本国公開実用新案公報 1971-2000年  
日本国実用新案登録公報 1996-2000年  
日本国登録実用新案公報 1994-2000年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

JICSTファイル (JOIS)

## C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	WO, 96/27155, A2 (InterTrust Technologies Corp.) 6. 9月. 1996 (06. 09. 96) & JP, 10-512074, A	1-15
Y	US, 6002771, A (Sun Microsystems, Incorporated) 22. 5月. 96 (22. 05. 96) & JP, 10-055383, A	1-15

☐ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの  
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの  
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)  
「O」 口頭による開示、使用、展示等に言及する文献  
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの  
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの  
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの  
「&」 同一パテントファミリー文献

国際調査を完了した日

19. 05. 00

国際調査報告の発送日

13. 06. 00

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号 100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

岩間 直純



5 L

9287

電話番号 03-3581-1101 内線 3562

**This Page Blank (uspto)**

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ BLACK BORDERS
- ☒ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☒ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**

**This Page Blank (uspto)**